Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

Problemas de Teoria dos Números

Dúnia Lisandra Serra Lêdo Pontes

Dissertação

MESTRADO EM MATEMÁTICA PARA PROFESSORES

2013

Universidade de Lisboa

Faculdade de Ciências

Departamento de Matemática

Problemas de Teoria dos Números

Dúnia Lisandra Serra Lêdo Pontes

Dissertação

MESTRADO EM MATEMÁTICA PARA PROFESSORES

Orientador: Professor Doutor Pedro Jorge Santos Freitas

2013

Resumo

A tese em questão, como o título sugere – *Problemas de teoria dos números* – propõe-se a estudar problemas relativos a uma das áreas mais antigas e mais ricas da matemática, considerada uma forte influência na evolução de grandes matemáticos.

Este trabalho conjuga dois temas deveras importantes para o desenvolvimento da criatividade e do conhecimento matemático: resolução de problemas e teoria dos números. A resolução de problemas é a força motora da progressão da Matemática enquanto ciência e a teoria dos números é uma fonte particularmente fértil de problemas interessantes e que são acessíveis a vários níveis.

Deste modo, pretende-se com este trabalho reunir alguns dos problemas de teoria dos números e, criar uma colecção que estimule o interesse dos alunos em Matemática e os incentive a participar em competições matemáticas.

Não é um objectivo desta tese ocupar-se de problemas impenetráveis, mas sim construir um manual de auxílio para um pequeno curso de resolução de problemas em teoria dos números, apresentando problemas mais simples, que qualquer aluno (pré-universitário) consiga resolver, e problemas de diferentes graus de dificuldade. A sequência de problemas está estruturada numa perspectiva evolutiva, começando por um capítulo dedicado a problemas que não envolvem técnicas especiais, seguido de um capítulo onde são apresentados teoremas úteis, e algumas demonstrações, para a resolução de problemas mais avançados, que são integrados no capítulo seguinte.

É ainda intenção desta tese explorar alguns dos mais importantes temas de teoria elementar dos números, focando especialmente em ideias cruciais para a resolução de problemas.

Ao longo deste trabalho expõem-se, comentam-se e resolvem-se problemas, escolhidos a pensar em alunos que desfrutam da Matemática e que simultaneamente tenham algum hábito de ler e compreender demonstrações.

Palavras-chave: teoria dos números, problemas, divisibilidade, primo, congruências.

(Não foi escrita ao abrigo do novo acordo ortográfico)

Agradecimentos

À minha família, que sempre apoiou todas as minhas decisões e que sempre se orgulhou do meu trabalho. Ao meu sobrinho que, apesar de ainda não ter consciência, é uma das pessoas que mais alegrias me dá.

Aos meus amigos por toda a paciência e encorajamento. Ao meu melhor amigo, Emanuel, por estar sempre presente e pelo bom humor contagiante.

A todos os professores do Mestrado em Matemática para Professores pelo conhecimento que partilharam comigo e pela dedicação demonstrada. À professora Carlota Gonçalves pela preocupação e atenção ao longo destes anos.

Ao professor Pedro Freitas pela compreensão, pela disponibilidade, pela força e coragem que me deu e por toda a sua sabedoria.

Índice

God created the integers, all else is the work of man.

Leopold Kronecker (1823-1891)

1. Introdução

A motivação para o tema desta tese – *Problemas de Teoria dos Números* – surgiu no decorrer do Mestrado de Matemática para Professores. A cadeira de Teoria e História dos Números fomentou o meu interesse pela teoria dos números, tendo sido inevitável escolher um assunto a desenvolver que incluísse esta temática. Por outro lado, a resolução de problemas sempre fez parte da minha visão da Matemática. O meu prematuro interesse pela Matemática e pelo ensino teve início com os jogos, problemas e puzles de que fui tendo conhecimento. Por isso, fez sentido para mim, que este mestrado, terminasse com uma abordagem a estes conteúdos.

Para a escolha deste tema, também foi importante o meu percurso profissional, que passou pelo ensino em diferentes escolas, consequentemente com alunos de diferentes capacidades, aptidões e interesses, e pelo trabalho numa editora de manuais escolares que visa, entre outros objetivos, ajudar os professores a estimular os seus alunos para a disciplina, apresentando aspectos atrativos da Matemática. Neste sentido, tenho sempre em mente o empenho, o progresso dos alunos em Matemática mas ao mesmo tempo o prazer que advém do conhecimento matemático.

O raciocínio e a lógica são, provavelmente, das capacidades mais importantes que podemos desenvolver com a Matemática, principalmente com a resolução de problemas.

Vejo esta tese de mestrado como uma oportunidade para pesquisar assuntos que sempre tive vontade de estudar mas que infelizmente pouco foram tratados ao longo da licenciatura e cujo escasso tempo das nossas vidas nos permite aprofundar.

O meu principal objectivo é criar um recurso útil para todos os professores ou alunos que vejam na Matemática um desafio, por vezes lúdico, mas com certeza sempre motivador e estimulante. Pretende-se ainda que este trabalho sirva como uma ferramenta para um pequeno curso em teoria dos números, ampliando a visão que os alunos têm da Matemática e, talvez, melhor prepará-los para uma possível participação em competições matemáticas, como é o exemplo das Olimpíadas Portuguesas de Matemática.

Pretendo ainda proporcionar o enriquecimento em algumas áreas da teoria dos números através da reorganização e otimização de estratégias dos alunos na resolução de problemas, bem como incentivar os alunos para a continuação dos estudos em Matemática.

A resolução de exercícios, apesar de necessária, principalmente no ensino básico, tem um poder limitado. Um exercício, muitas vezes, é uma pergunta que se limita a testar os conhecimentos recentemente assimilados. Os exercícios podem ser fáceis ou difíceis, mas nunca são enigmáticos (*puzzling*), sendo facilmente percetível o procedimento a aplicar. Um problema é o oposto, é uma pergunta cuja resposta não pode ser obtida imediatamente, pode até ser não ter solução e muitas vezes requere alguma pesquisa antes de se chegar à solução. A investigação em Matemática resume-se á resolução de problemas em aberto e,

consequentemente, pode dizer-se que os problemas e a resolução de problemas estão no centro da Matemática.

Alguém que é capaz de resolver problemas em Matemática desenvolve confiança e poderá inspirar outros a seguir o seu exemplo. E acima de tudo, resolver problemas é um divertimento, permitindo compreender e apreciar a beleza da Matemática.

A minha fascinação pela resolução de problemas prende-se com a capacidade que um problema tem em captar a minha atenção e incentivar-me a desenvolver um trabalho que, para qualquer outra pessoa, poderá parecer árduo (e talvez inútil), mas que para mim será uma conquista.

É de referir, que a inscrição neste mestrado foi puramente opcional e uma escolha pessoal, devido à necessidade que sentia em completar a minha formação inicial. Uma possibilidade para obter conhecimentos e instrumentos que me permitissem aperfeiçoar o meu trabalho. E se o meu maior objetivo com a frequência deste mestrado é adquirir mais conhecimentos, penso ser importante, a espírito de introdução, pesquisar um pouco sobre a história da teoria dos números.

Fazer uma contextualização histórica da teoria dos números pode tornar-se um trabalho ingrato, no sentido em que esta área matemática é tão antiga e tão vasta, sendo quase impossível fazer uma abordagem concisa e resumida sem deixar de mencionar algumas situações importantes.

Deste modo, farei uma breve incursão na história da matemática de modo a apresentar alguns exemplos que permitam perceber a origem e evolução da teoria dos números, com o objetivo de melhor compreender este tema, apesar de não ter a intenção de fazer um desenvolvimento histórico exaustivo deste assunto.

1.1. Breve incursão na História da Matemática

A teoria dos números, ao longo do tempo, tem fascinado tanto amadores como profissionais, talvez mais do que qualquer outro ramo da Matemática.

A necessidade de contar, presente nas civilizações mais antigas, impulsionou o surgimento dos números naturais e está na origem da teoria dos números.

Assim, o objeto de estudo desta área matemática acompanha a humanidade desde sempre, e ao longo da história das civilizações foi sendo feito o estudo das propriedades e relações entre os números inteiros, mesmo que ainda não de um modo formal.

Povos como os egípcios ou os babilónios criaram formas de representação dos números naturais e modos de os operar. Até aos nossos dias chegaram-nos registos de relações descobertas por estes povos, como é o caso da tábua Plimpton, escrita pelos babilónios por volta de 1900 a 1600 a. C., onde estão registados os ternos designados atualmente por ternos pitagóricos, por satisfazerem o conhecido teorema de Pitágoras; ou o caso do papiro de Rhind, um documento egípcio escrito cerca de 1650 a. C, com informações sobre aritmética, fracções, cálculo de áreas, volumes, entre muitos outros temas.

Para os gregos a palavra «número» referia-se apenas aos números inteiros. Os pitagóricos estudaram as propriedades dos números, e a eles é atribuído, por exemplo, o conceito de número perfeito: um número cuja soma dos seus divisores próprios é igual ao próprio número.

Três dos livros da obra *Elementos*, de Euclides, contêm um total de 102 proposições que trabalham essencialmente com a natureza e as propriedades dos números naturais. Nestes livros encontram-se, por exemplo: a definição de número primo e uma demonstração, ainda hoje utilizada, da infinidade dos números primos; o algoritmo para calcular o máximo divisor comum de dois números, hoje conhecido por algoritmo de Euclides e o estudo de números perfeitos.

Diofanto (século III) foi outro matemático grego importante que influenciou outros grandes matemáticos na exploração e desenvolvimento da teoria dos números. Fermat (1601-1665) foi um dos matemáticos a interessar-se pela obra de Diofanto, tendo escrito numa das margens do livro de autoria de Diofanto, *Aritmética*, que tinha conseguido provar que não há soluções inteiras da equação $x^n + y^n = z^n$ quando $n \geq 3$. Esta demonstração não chegou a ser conhecida, pois Fermat afirmou não ter espaço para a incluir na referida margem. Este resultado ficou conhecido como o Último Teorema de Fermat e apenas foi demonstrado em 1994 pelo matemático Andrew Wiles. Mais uma vez, Fermat tinha razão, pois a demonstração tem cerca de 125 páginas…

Euler, Lagrange, Gauss são outros exemplos de nomes sonantes da matemática que desenvolveram o seu trabalho na área da teoria dos números.

Actualmente, a teoria dos números é uma área da matemática com vários resultados importantes, tendo grande impacto no desenvolvimento de outras áreas matemáticas.

> *Mathematics is the Queen of the sciences, and the theory of numbers is the Queen of mathematics.*
>
> Gauss

É de referir que ao longo do trabalho o conjunto dos números inteiros (positivos e negativos, incluindo o zero) será denotado por $\mathbb{Z}$ e o conjunto dos números naturais (apenas inteiros positivos) por $\mathbb{N}$. Se nada for dito em contrário assumimos que qualquer letra do alfabeto, de a a z, representa um número inteiro, reservando as letras p e q para representar números primos.

2. Problemas que não envolvam técnicas especiais

Neste capítulo pretende-se abordar problemas cuja resolução não exija nenhuma técnica avançada. Praticamente todos os temas trabalhados neste capítulo são estudados, provavelmente não de forma tão aprofundada, no Ensino Básico ou Secundário, permitindo que as resoluções tenham uma abordagem próxima dos conhecimentos dos alunos.

Divisibilidade

Sejam a, b inteiros, dizemos que b é **divisível** por a, ou a divide b, se existe um inteiro c tal que $b = ac$, isto é, $\frac{b}{c}$ é inteiro. Denota-se por $a|b$. Neste caso, também se diz que b é múltiplo de a e que a é divisor de b.
Se b é não é divisível por a então escrevemos $a \nmid b$ (ou seja, não existe c nas condições referidas).

Temos ainda que: $a|0$ para qualquer inteiro a, pois $0 = 0 \cdot a$; e $0 \nmid b$ para todo $b \neq 0$ pois $b \neq 0 = 0 \cdot a$, qualquer que seja a.

A partir da definição de divisibilidade é possível obter algumas propriedades simples.

1. $1|a$, $a|a$
2. $a|1 \Rightarrow a = \pm 1$
3. $a|b$ e $c|d$ então $ac|bd$
4. $a|b$ e $b|c$ então $a|c$
5. $a|b$ e $b|a$ então $a = \pm b$
6. $a|b$ e $b \neq 0$ então $|a| \leq |b|$
7. $a|b$ e $a|c$ então $a|(xb + yc)$ para x, y inteiros
8. $a|(b + c)$ e $a|b$ então $a|c$
9. $a|b$ então $a|bc$ e ainda $ac|bc$
10. $a|b$ e $b \neq 0$ então $\frac{b}{a}|b$
11. $a|b \Leftrightarrow ac|bc$ para qualquer que seja $c \neq 0$

Seja $a \in \mathbb{Z}$, dizemos que a é **par** se $2|a$ e que a é **ímpar** se $2 \nmid a$.
Assim, o conjunto dos números inteiros pode ser dividido em dois subconjuntos, o conjunto dos números pares e o conjunto dos números ímpares:

$\{0, \pm 2, \pm 4, \dots\}$ e $\{\pm 1, \pm 3, \pm 5, \dots\}$, respectivamente.

Observações.

1. Todo o número par é da forma $2k$, $k \in \mathbb{Z}$
2. Todo o número ímpar é da forma $2k+1$, $k \in \mathbb{Z}$

Problema 2.1. Vinte alunos estão num corredor com cacifos numerados de 1 a 20. O primeiro aluno abre todos os cacifos; o segundo fecha os cacifos com números pares; o terceiro muda o estado das portas dos cacifos numerados com múltiplos de 3, ou seja, se a porta está fechada ele abre, se está fechada ele abre; e assim sucessivamente até ao vigésimo aluno. No final quantos cacifos ficam abertos?

Resolução:

Vamos resolver este problema de duas formas diferentes. A primeira resolução será feita recorrendo a um esquema e é acessível a qualquer aluno com algumas bases de matemática, enquanto a segunda resolução irá utilizar uma das propriedades anteriores. Contudo, é óbvio que a primeira resolução é limitada, pois se o número de cacifos for maior, o esquema deixa de ser viável.

1.ª resolução:

Se o n-ésimo aluno, apenas, altera o estado dos cacifos numerados com múltiplos de n, então abre ou fecha as portas dos cacifos com números m tais que $n|m$. Assim, é fácil verificar que o estado de cada cacifo será alterado tantas vezes quanto o número de divisores do respectivo número.

Como inicialmente os cacifos estão fechados, sabemos que ficam abertos os cacifos cujo estado da porta for alterado um número ímpar de vezes, isto é, os cacifos cujo número de divisores for ímpar.

Façamos, então, uma tabela com os divisores de cada número de 1 a 20.

n.º cacifo	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
divisores (n-ésimo aluno)	1	1, 2	1, 3	1, 2, 4	1, 5	1, 2, 3, 6	1, 7	1, 2, 4, 8	1, 3, 9	1, 2, 5, 10
n.º cacifo	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
divisores (n-ésimo aluno)	1, 11	1, 2, 3, 4, 6, 12	1, 13	1, 2, 7, 14	1, 3, 5, 15	1, 2, 4, 8, 16	1, 17	1, 2, 3, 6, 9, 18	1, 19	1, 2, 4, 5, 10, 20

Pela tabela, observamos que o estado dos cacifos numerados com 1, 4, 9 e 16 é alterado um número ímpar de vezes e por isso serão 4 os cacifos com as portas abertas no final.

2.ª resolução:

Pela propriedade 10, verificamos que qualquer inteiro $b \neq 0$ tem um número par de divisores positivos, excepto se b for um quadrado perfeito, isto é, se existir um inteiro a tal que $b = a^2$.

Isto acontece porque para cada divisor a, de b, $\frac{b}{a}$ também divide b, logo se $a \neq \frac{b}{a}$ os divisores de b surgem aos pares. No caso de $a = \frac{b}{a}$ então $b = a^2$ e, portanto, b é um quadrado perfeito.

Como foi visto na primeira resolução, estamos à procura dos cacifos cujo número de divisores seja ímpar, ou seja, os cacifos numerados com quadrados perfeitos: $1 = 1^2$, $4 = 2^2, 9 = 3^2$ e $16 = 4^2$.

Contundo, para quaisquer dois inteiros a e b, nem sempre b é divisível por a. Vamos, assim, introduzir um resultado que tem um papel importante na teoria dos números: o algoritmo da divisão.

Algoritmo da Divisão

Sejam a e b inteiros, com $b > 0$ então existe um único par (q, r) de números inteiros tal que,

$$a = bq + r \text{ e } 0 \leq r < b$$

Dizemos que q é o **quociente** e r o **resto** da divisão de a por b.

Problema 2.2. Prova que o número $n^3 + 2n$ é divisível por 3, para qualquer natural n.

Resolução:

Nesta resolução partimos do princípio de que os restos da divisão de n por 3 só podem ser iguais a 0, 1 ou 2.

Para facilitar os cálculos, consideremos $n = 3k + r$ com $r = 0, 1, 2$.

$$\begin{aligned} n^3 + 2n &= (3k + r)^3 + 2(3k + r) \\ &= (9k^2 + 6rk + r^2)(3k + r) + 6k + 2r \\ &= 27k^3 + 27rk^2 + (9r^2 + 6)k + (r^3 + 2r) \end{aligned}$$

Obtida a expressão anterior, analisaremos cada um dos casos.

- Se $r = 0$,

$$n^3 + 2n = 27k^3 + 27 \times 0 \times k^2 + (9 \times 0^2 + 6)k + (0^3 + 2r)$$
$$= 27k^3 + 6k = 3\underbrace{(9k^3 + 2k)}_{\in \mathbb{Z}}$$

Logo, $n^3 + 2n$ é divisível por 3.

- Se $r = 1$,

$$n^3 + 2n = 27k^3 + 27 \times 1 \times k^2 + (9 \times 1^2 + 6)k + (1^3 + 2r)$$
$$= 27k^3 + 27k^2 + 15k + 3 = 3\underbrace{(9k^3 + 9k^2 + 5k + 1),}_{\in \mathbb{Z}}$$

Logo, $n^3 + 2n$ é divisível por 3.

- Se $r = 2$,

$$n^3 + 2n = 27k^3 + 27 \times 2 \times k^2 + (9 \times 2^2 + 6)k + (2^3 + 2r)$$
$$= 27k^3 + 54k^2 + 42k + 12 = 3\underbrace{(9k^3 + 18k^2 + 14k + 4)}_{\in \mathbb{Z}}$$

Logo, $n^3 + 2n$ é divisível por 3.

Números Primos

Seja $p \in \mathbb{N}$, diz-se que p é **primo** se for divisível apenas por 1 e por p, com $p > 1$. Isto é, o inteiro $p > 1$ é primo se não existir nenhum inteiro d com $d > 1$ e $d \neq p$ tal que $d|p$.

Os primeiros números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, sendo 2 o único primo par.

Um número inteiro $n > 1$ que não seja primo é designado de **composto**. Eratóstenes observou que todo número composto é divisível por qualquer primo menor ou igual à sua raiz quadrada, ou seja, existe p primo tal que $p|n$ e $p \leq \sqrt{n}$.

Por exemplo, será 53 primo ou composto? Como $\sqrt{53} \approx 7{,}28$, sabemos que 53 é primo se não for divisível por 2, 3, 5 e 7. De facto, nenhum destes números primos divide 53, logo 53 também é primo.

Observações.

1. O número 1 não é nem primo nem composto.
2. Existe uma infinidade de números primos.

dem: Suponhamos que existe um número finito n de primos, $p_{1,}p_2, \dots, p_n$com $p_1 < p_2 < \cdots < p_n$. Consideremos o número $N = p_1p_2 \cdots p_n + 1$. Se N for primo, temos que existem pelo menos $n+1$ primos, pois $N > p_n$, o que contradiz a hipótese. Então N é composto, e por isso existe p primo, de entre os primos $p_{1,}p_2, \dots, p_n$, tal que $p|N$. Seja $p = p_k$, com $1 < k < n$, então p_k divide $p_1p_2 \cdots p_n + 1$. É óbvio que p_k divide $p_1p_2 \cdots p_n$e, pela propriedade 8 da divisibilidade, temos que $p_k|1$, chegando assim a outra contradição pois p_ké primo e logo maior do que 1. ■

Problema 2.3. Sejam p e q dois inteiros primos. Sabendo que a equação $x^2 - px + q = 0$ tem duas raízes inteiras distintas, descobre p e q.

Resolução:

Sejam x_1 e x_2 as duas raízes da equação dada. Sendo as raízes distintas suponhamos que $x_2 > x_1$.

Então, podemos escrever

$$x^2 - px + q = (x - x_1)(x - x_2) = x^2 - \underbrace{(x_1 + x_2)}_{p} x + \underbrace{x_1x_2}_{q}$$

Apesar de não constar do programa de Matemática, ao estudar a fórmula resolvente no Ensino Básico, este resultado referente à soma e ao produto das raízes de uma equação do 2.º grau é, geralmente, abordado.

Assim, temos que $p = x_1 + x_2$ e $q = x_1x_2$.

Como q é primo e $x_2 > x_1$ então $x_1 = 1$ e $x_2 = q$. Logo, $p = 1 + q$ e, portanto, p e q são primos consecutivos. Os menores primos nestas condições são 2 e 3, ou seja, $p = 3$ e $q = 2$.

Nota: não há mais primos consecutivos, pois dados quaisquer dois números consecutivos, um deles é par e 2 é o único primo par.

Ainda, p primo dizemos que p^k divide completamente n se k for o maior natural tal que $p^k|n$, e escreve-se $p^k \parallel n$. Por exemplo, $3^2 \parallel 18$ e $2^2 \nparallel 24$.

Teorema Fundamental da Aritmética

É trivial perceber que um número composto pode ser escrito como o produto de dois números naturais diferentes de 1 e de ele próprio. Por exemplo, 90 é composto porque pode ser representado por $90 = 5 \times 18$. Mas, neste produto, surge o 18 que também é composto pois $18 = 3 \times 6$ e por isso $90 = 5 \times 3 \times 6$. Se observamos este último produto, ainda podemos escrever o 6 como produto de 2 por 3. Assim, temos $90 = 5 \times 3 \times 2 \times 3$, obtendo um produto com apenas números primos.

Aplicando este raciocínio, percebe-se facilmente, que podemos decompor num produto de factores cada vez menores qualquer número natural maior do que 1.

Voltando ao exemplo, e se tivéssemos escrito primeiro $90 = 2 \times 45$, obteríamos a mesma decomposição em factores? A resposta, é sim. Apenas teríamos os factores escritos por uma ordem diferente, por exemplo $90 = 2 \times 5 \times 9 = 2 \times 5 \times 3 \times 3$, e por isso verificamos que a decomposição em factores primos é a mesma em ambos os casos.

Este é um exemplo simples e muito próximo do que os alunos aprendem no Ensino Básico que conduz a um teorema muito importante na Teoria dos Números.

Teorema Fundamental da Aritmética (TFA) diz que todo o número natural maior do que 1 se factoriza como produto de primos e os primos que aparecem na factorização são bem determinados, isto é, tem uma única representação como produto de números primos.

Demonstremos então o teorema.

A demonstração apresentada da existência consiste num método que se designa por *indução forte* em que o objectivo é provar que a proposição $P(n)$ é verdadeira para todo n, utilizando a indução em n. Assim, primeiro é necessário mostrar que $P(1)$ é verdadeira e, de seguida, supondo que as proposições $P(1)$, …, $P(n-1)$ são verdadeiras, provar que a proposição $P(n)$ também é verdadeira.

dem:

Existência

O resultado é verdadeiro para $n = 2$, pois 2 é um número primo e por isso $n = 2$ é a sua factorização.

Suponhamos que o resultado é verdadeiro para todos os naturais menores que n e vamos mostrar que também é verdadeiro para n. Se n for um número primo então existe p_1 primo tal que a decomposição em factores primos de n seja $n = p_1$. Se n for composto podemos escrever $n = ab$, com a e b diferentes de 1 e de n. Como $a, b < n$, por hipótese de indução a e b admitem decomposição em factores primos. O produto das decomposição em factores primos de a e b dá-nos a decomposição em factores primos de n. ■

Provavelmente, muitos consideram trivial a existência da decomposição em factores primos, principalmente depois de observar um caso concreto como o que foi apresentado. Mas, talvez, o mesmo não aconteça com a unicidade. Na verdade, a unicidade não é tão simples quanto parece ser. Vejamos um exemplo de como a unicidade não pode ser dada como "garantida".

Consideremos o seguinte problema:

Sejam $x, y \in \mathbb{N}$ *tal que* $5x = 3y$. *Será que podemos afirmar que* $3|x$ *e* $5|y$*?*

Pela igualdade, verificamos que $5x$ é múltiplo de 3 e como 3 e 5 são números primos distintos então x tem de ser múltiplo de 3, ou seja, x tem de conter o 3 na sua decomposição em factores primos. Este raciocínio só é possível devido ao Teorema Fundamental da Aritmética, pois caso a decomposição em factores primos não fosse única seria possível um número ser decomposto em factores de uma determinada forma e ter um 5 como um factor primo mas sem nenhum 3, e quando decomposto em factores de outra forma não ter nenhum factor igual a 5 mas ter um factor 3.

Por exemplo, consideremos o conjunto dos números naturais pares $2\mathbb{N} = \{0, 2, 4, \dots\}$. Definimos primo neste conjunto como um número que não admite decomposição em factores primos dentro do conjunto. Nestas condições, por exemplo,6 é um número primo mas 8 não é. De facto, nas duas possíveis decomposições em factores de 6, $6 = 2 \times 3$ e $6 = 6 \times 1$, há elementos ímpares, isto é, que não pertencem a $2\mathbb{N}$. O número 8 não é primo porque podemos escrever 8 como um produto de dois números pares, $8 = 2 \times 4$.

Deste modo, existem sistemas que admitem a decomposição em factores em primos mas onde não se verifica a unicidade. Por exemplo, como os números $2, 6, 10$ e 30 são primos em $2\mathbb{N}$, o número 60 tem duas decomposições em factores primos diferentes:

$$60 = 2 \times 30 = 6 \times 10$$

Assim, não se verifica a unicidade em $2\mathbb{N}$. Logo, se $x, y \in 2\mathbb{N}$ tal que $2x = 10y$, não podemos concluir que $10|x$ e $2|y$, apesar de 2 e 10 serem primos, pois em $2\mathbb{N}$ temos que $10 \nmid 30$ nem $2 \nmid 10$.

Portanto, a questão relativa à unicidade é mais complexa do que parece e por isso iremos demonstrá-la mais à frente depois de serem estudados alguns resultados que simplificam a compreensão da prova.

Deste teorema (TFA) podemos ainda verificar que qualquer natural $n \geq 1$ se escreve de forma única como,

$$\boldsymbol{n = p_1^{k_1} \dots p_r^{k_r}} \quad \text{com } p_1, \dots, p_r \text{ primos distintos e } k_1, \dots, k_r \geq 1$$

A esta representação chamamos **factorização** de n. Note-se que a factorização do produto de dois números naturais maiores do que 1 é igual ao produto da factorização de cada um dos números.

O resultado seguinte será utilizado na resolução dos exemplos apresentados. A sua demonstração é simples mas o raciocínio aplicado é importante para obter a solução dos referidos exemplos.

Sejam a e b inteiros e p primo. Se $p|ab$ então $p|a$ ou $p|b$.

dem:

Se p divide ab então p é um dos factores da factorização de ab. Como a factorização de ab é igual ao produto das factorizações de a e b, e estas são únicas, então p tem de fazer parte de pelo menos uma das factorizações a e b.

Por indução se verifica que se $p|a_1 \dots a_2$ então $p|a_i$ para algum i.

Problema 2.4.

4.1. O produto $2^9 \cdot 3$ é divisível por 8? E por 9?

4.2. Verdadeiro ou falso? *Qualquer número natural que seja divisível por* 4 *e por* 6 *é divisível por* $4 \times 6 = 24$.

Resolução:

4.1. Para $2^9 \cdot 3$ ser divisível por 8 é necessário que na factorização de $2^9 \cdot 3$ apareçam pelo menos três factores iguais a 2, pois $8 = 2^3$. Logo, $2^9 \cdot 3$ é divisível por 8 porque na sua factorização existem nove factores 2.

Na factorização de $2^9 \cdot 3$ existe apenas um factor 3, mas $9 = 3^2$. Logo, $2^9 \cdot 3$ não é divisível por 9.

4.2. Seja n natural tal que $4|n$ e $6|n$. Como $4 = 2^2$ e $6 = 2 \times 3$ então na factorização de n existem, pelo menos, dois factores iguais a 2 e um factor 3. No entanto, $24 = 2^3 \times 3$, logo para n ser divisível por 24 a sua factorização tem de ter pelo menos três factores 3.

Facilmente encontramos um contra-exemplo. Se considerarmos $n = 12 = 2^2 \times 3$ então n é divisível por 4 e por 6 mas não é divisível por 24.

Máximo Divisor Comum e Mínimo Múltiplo Comum

A noção de máximo divisor comum, tal como a de mínimo múltiplo comum, é trabalhada desde cedo, no 1.º ciclo, apesar da introdução formal destes conceitos só ser feita no 2.º ciclo.

Sejam a e b dois inteiros. Dizemos que $d > 0$ é o **máximo divisor comum** de a e b se:

i. $d|a$ e $d|b$
ii. $c|a$ e $c|b$ então $c \leq d$, para todo c.

Escreve-se $d = \text{mdc}(a, b)$.

Observações. É imediato que:

1. $\text{mdc}(a, b) = \text{mdc}(b, a)$
2. $\text{mdc}(a, 1) = 1$

3. mdc(0, 0) não existe
4. $\text{mdc}(a, 0) = |a|$
5. Se $a|b$, então $\text{mdc}(a, b) = |a|$
6. Se p primo então $\text{mdc}(p, a) = p$ ou $\text{mdc}(p, a) = 1$
7. Todos os divisores comuns de a e b dividem $\text{mdc}(a, b)$

Sejam a e b dois inteiros. Dizemos que $m > 0$ é o **mínimo múltiplo comum** de a e b se:

i. $a|m$ e $b|m$
ii. Se m' for outro múltiplo comum de a e b, então $m' \geq m$.

O mínimo múltiplo comum de a e b, é o menor inteiro positivo que é divisível por a e b.

Escreve-se $m = \text{mmc}(a, b)$.

Observações. É imediato que:

1. $\text{mmc}(a, b) = \text{mmc}(b, a)$
2. $\text{mmc}(a, 1) = a$
3. mmc(0, 0) não existe
4. $\text{mmc}(a, 0)$ não existe
5. Se $a|b$, então $\text{mmc}(a, b) = b$
6. $\text{mmc}(a, b)$ divide todos os múltiplo comuns de a e b

É de referir que ambas as definições de mdc e mmc podem ser estendidas para mais do que dois números:

- $\text{mdc}(a_1, a_2, \dots, a_n)$ é o maior natural de entre todos os divisores comuns a $a_1, a_2, \dots, a_n$.
- $\text{mmc}(a_1, a_2, \dots, a_n)$ é o menor natural de entre todos os múltiplos comuns a $a_1, a_2, \dots, a_n$.

Problema 2.5. Dados os números $\text{A} = 2^3 \times 3^{10} \times 5 \times 7^2$ e $\text{B} = 2^5 \times 3 \times 11$, sem calcular os valores de A e B, determina $\text{mdc}(\text{A}, \text{B})$.

Resolução:

Seja d um divisor comum de A e B, então a factorização de d é dada pelo produto dos números primos que constam, simultaneamente, das factorizações de A e B, ou seja, 2 e 3 (por exemplo, se na factorização de d existir algum factor que não faça parte da factorização de A então d não pode dividir A).

Assim, podemos escrever $d = 2^{k_1} \times 3^{k_2}$, com $k_1, k_2 \geq 1$. Como na factorização de A existem apenas três factores 2, então $1 \leq k_1 \leq 3$, caso contrário $d \nmid$ A; analogamente, porque existe apenas um factor 3, na factorização de B, então $k_2 = 1$, caso contrário $d \nmid$ B.

Como procuramos o máximo divisor comum pretende-se obter o maior valor de d, logo, $d = 2^3 \times 3 = 24$.

Problema 2.6. Dados os números $A = 2^2 \times 5^3 \times 7^2$ e $B = 2^5 \times 3 \times 5$, sem calcular os valores de A e B, determina $\text{mmc}(A, B)$.

Resolução:

A resolução deste problema é análoga ao problema **5**. Neste caso, a factorização de m, o mínimo múltiplo comum, tem de incluir todos os factores que constam das factorizações de A e B, elevados ao maior expoente. É de notar que o mmc não necessita de incluir mais nenhum factor pois caso incluísse deixava de ser o menor múltiplo comum. Logo $\text{mmc}(A, B) = 2^5 \times 3 \times 5^3 \times 7^2 = 588000$.

Problema 2.7. Encontra o menor número natural que tem resto 1 quando dividido por 2, resto 2 quando dividido por 3, resto 3 quando dividido por 4, resto 4 quando dividido por 5 e resto 5 quando dividido por 6.

Resolução:

Seja n o número que procuramos, então podemos representar de cinco formas diferentes:

$n = 2k_1 + 1;\ n = 3k_2 + 2;\ n = 4k_3 + 3;\ n = 5k_4 + 4;\ n = 6k_5 + 5$

Observando as diferentes representações verifica-se que $n + 1$ é múltiplo de 2, 3, 4, 5 e 6, e o menor valor é dado por $n + 1 = \text{mmc}(2, 3, 4, 5, 6)$.

Temos que 2, 3 e 5 são números primos e $4 = 2^2$ e $6 = 2 \times 3$, logo

$$n + 1 = \text{mmc}(2, 3, 4, 5, 6) = 2^2 \times 3 \times 5 = 60.$$

Portanto, $n = 59$.

Dos problemas **5** e **6**, podemos generalizar e escrever o que se segue.

Dados dois números $m, n \in \mathbb{N}$ se $m = {p_1}^{t_1} \ldots {p_r}^{t_r}$ e $n = {p_1}^{s_1} \ldots {p_r}^{s_r}$, com $t_i, s_i \geq 0, i = 1, \ldots, k$, então:

$$\text{mdc}(m, n) = {p_1}^{\min(t_i, s_i)} \ldots {p_r}^{\min(t_i, s_i)}$$

tal como

$$\text{mmc}(m, n) = {p_1}^{\max(t_i, s_i)} \ldots {p_r}^{\max(t_i, s_i)}$$

É também útil conhecer a seguinte relação entre o máximo divisor comum e o mínimo múltiplo comum de dois números naturais:

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = ab$$

Esta relação não é facilmente generalizada para mais de dois naturais. Por exemplo, para o caso de três números a igualdade nem sempre é verificada:

$$\text{mdc}(6, 18, 24) \cdot \text{mmc}(6, 18, 24) = 6 \times 72 = \mathbf{432} \neq \mathbf{2592} = 6 \times 18 \times 24$$

Algoritmo de Euclides

A factorização de números permite-nos determinar o máximo divisor comum de dois números. Contudo para números muito grandes pode não ser exequível, pelo menos sem um computador. Para alguém que tenha dúvidas, tente calcular o máximo divisor comum de 1381955 e 690713.

O algoritmo de Euclides é um método para a determinação do máximo divisor comum de dois números naturais e destaca-se por ser simples e eficiente. Trata-se de um dos mais antigos algoritmos conhecidos, apresentado na obra *Elementos* do matemático Euclides (325 a. C.-265 a. C.) e, ainda hoje, é utilizado e ensinado nas escolas. Por requerer apenas a divisão inteira constitui um processo acessível e prático.

O algoritmo de Euclides baseia-se no seguinte: pelo algoritmo da divisão podemos escrever $a = bq + r$. Então $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.

Isto é,

$$d|a \text{ e } d|b \Leftrightarrow d|b \text{ e } d|r$$

dem:

(⇒) Suponhamos que $d|a$ e $d|b$.

$$a = bq + r \Leftrightarrow r = a - bq$$

Por hipótese $d|a$ e $d|b$, logo pela propriedade 9 da divisibilidade $d|bq$ e pela propriedade 7 $d|a - bq$, ou seja, $d|r$.

(⇐) Suponhamos que $d|b$ e $d|r$.

$$a = bq + r$$

Com um raciocínio análogo ao anterior, temos que $d|a$.

Assim, $\mathrm{mdc}(a, b)$ e $\mathrm{mdc}(b, r)$ são definidos como máximos do mesmo conjunto, logo são iguais. ■

O **algoritmo de Euclides** consiste na aplicação repetida do algoritmo da divisão:

Sejam a, $b \in \mathbb{N}$, pelo algoritmo da divisão

$$\exists q_1, r_1 \text{ tais que } a = bq_1 + r_1, 0 \leq r_1 \leq b$$

Se $r_1 = 0$ então o processo termina.

Se $r_1 \neq 0$,

$$\exists q_2, r_2 \text{ tais que } b = r_1 q_2 + r_2, 0 \leq r_2 \leq r_1$$

Se $r_2 = 0$ então o processo termina.

Se $r_2 \neq 0$,

$$\exists q_3, r_3 \text{ tais que } r_1 = r_2 q_3 + r_3, 0 \leq r_3 \leq r_2$$

Se $r_3 = 0$ então o processo termina.

$\vdots$

Se $r_k \neq 0$,

$$\exists q_{k+1}, r_{k+1} \text{ tais que } r_{k-1} = r_k q_{k+1} + r_{k+1}, 0 \leq r_{k+1} \leq r_k$$

Esta cadeia de igualdades é finita porque $b > r_1 > r_2 > \cdots > r_k > r_{k+1} \geq 0$.
Logo, existe $s \in \mathbb{N}_0$ tal que $r_s \neq 0$ porém $r_{s+1} = 0$.

Assim, aplicando sucessivamente a igualdade, anteriormente provada, $\text{mdc}(a, b) = \text{mdc}(b, r)$ em que $a = bq + r$, obtemos

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{s-1}, r_s) = r_s$$

Problema 2.8. Prova que, para todo o natural n, a fracção $\frac{12n+1}{30n+2}$ é irredutível.

Resolução:

Uma fracção é irredutível se não existe nenhum divisor comum ao numerador e denominador, isto é, se o máximo divisor comum entre os da fracção for igual a 1.

Assim, basta determinar $\text{mdc}(30n + 2, 12n + 1)$ e verificar que é igual a 1.

Utilizando o algoritmo de Euclides:

$30n + 2$	$12n + 1$	$12n + 1$	$6n$	$6n$	1
$-24n - 2$	2	$-12n$	2	$-6n$	1
$6n$		1		0	

Isto é, $\text{mdc}(30n + 1, 12n + 1) = \text{mdc}(12n + 1, 6n) = \text{mdc}(6n, 1) = 1$.

Voltemos algoritmo de Euclides para determinar $\text{mdc}(360, 75)$.

275	120	120	35	35	15	15	5
35	2	15	3	5	2	0	3

Assim, $\text{mdc}(275,120) = \text{mdc}(120,35) = \text{mdc}(35,15) = \text{mdc}(15,5) = 5$.

A partir das divisões efectuadas é possível escrever três igualdades que permitirão a escrita do $\text{mdc}(275,120)$ como uma combinação linear de 275 e 120, isto é, será possível escrever 5 na forma $275x + 120y$.

O $\text{mdc}(275,120)$ resultou do algoritmo de Euclides como o último resto diferente de zero, logo podemos exprimir 5 como combinação linear de 35 e 15. Iniciamos o processo por esta igualdade, fazendo, de seguida, sucessivas substituições com as outras duas igualdades.

$$
\begin{aligned}
5 &= 35 - 15 \times 2 \\
5 &= 35 - (120 - 35 \times 3) \times 2 \qquad \leftarrow\ 15 = 120 - 35 \times 3 \\
5 &= 35 - (120 \times 2 - 35 \times 6) \\
5 &= 35 \times 7 - (120 \times 2) \\
5 &= (275 - 120 \times 2) \times 7 - (120 \times 2) \qquad \leftarrow\ 35 = 275 - 120 \times 2 \\
5 &= 275 \times 7 - 120 \times 14 - 120 \times 2 \\
5 &= 275 \times 7 - 120 \times 16 \\
5 &= 275 \times 7 + 120 \times (-16)
\end{aligned}
$$

Portanto, podemos escrever $5 = 275x + 120y$, com $x = 5$ e $y = -16$.

Identidade de Bézout diz que se $d = \text{mdc}(a,b)$, então existem inteiros x, y tais que $d = ax + by$.

Seja $S = \{ax + by : x, y \text{ inteiros}\}$. Os elementos se S são exactamente os múltiplos de $d = \text{mdc}(a,b)$. Em particular,

$$\min(S \cap \mathbb{N}) = \text{mdc}(a,b)$$

dem:

Pela Identidade de Bézout sabemos que $d = \text{mdc}(a,b) \in S$. Queremos provar que os restantes elementos de S são múltiplos de d.

Se $d|d'$ então existe $k \in \mathbb{Z}$ tal que $d' = kd$.

Como $d = ax_0 + by_0$ temos que $d' = kd = a(kx_0) + (ky_0)b$, logo $d' \in S$.

Reciprocamente, seja $d' = ax + by \in S$, queremos mostrar que $d|d'$.

Como $d|a$ e $d|b$ então $d|(ax + by)$, isto é, d' é múltiplo de d. ■

A equação $ax + by = c$ tem soluções inteiras se e só se $\text{mdc}(a,b)|c$.

Os inteiros a, b dizem-se primos entre si ou **coprimos** se $\text{mdc}(a,b) = 1$.

Por exemplo, 8 e 3, 9 e 2, 5 e 7, são coprimos. Aliás, facilmente se percebe que quaisquer dois de números primos são coprimos, assim como quaisquer dois números consecutivos.

Expomos de seguida algumas propriedades dos números coprimos.

Os números a e b são coprimos se e só se $1 = ax + by$.

dem:

Se a e b forem coprimos então $1 = \text{mdc}(a, b)$. Logo, $1 = ax + by$.

Reciprocamente, se $1 = ax + by$ então 1 é múltiplo de $\text{mdc}(a, b)$. Logo, $1 = \text{mdc}(a, b)$.

Se $d = \text{mdc}(a, b)$, então $\frac{a}{d}$ e $\frac{b}{d}$ são coprimos.

dem:

Pela identidade de Bézout temos $d = ax + by$.

Dividindo ambos os membros da equação por d, obtemos $1 = \frac{a}{d}x + \frac{b}{d}y$.

Logo, $1 = \text{mdc}(\frac{a}{d}, \frac{b}{d})$.

Lema de Euclides. Sejam a e b são coprimos e $a|bc$ então $a|c$.

dem:

Como a e b são coprimos então $1 = ax + by$. Multiplicando ambos os membros da equação por c, obtemos $c = acx + bcy$.

Mas $a|acx$ e por hipótese $a|bc$ logo $a|bcy$. Portanto, $a|\ (acx + bcy)$, ou seja, $a|c$. ■

Sejam a e b coprimos. Se $a|c$ e $b|c$ então $ab|c$.

dem:

Como $a|c$ temos que $c = ak$ para um certo k inteiro. Mas $b|c$ logo $b|ak$.

Como a e b são coprimos pelo Lema de Euclides temos que $b|k$, ou seja, $k = bx$ para um certo x inteiro. Assim, podemos escrever $c = abx$ e, portanto, $ab|c$. ■

Vejamos o seguinte exemplo:

Consideremos os números 4 e 6. O máximo divisor comum destes dois números é 2 e por isso não são coprimos. Temos, por exemplo, que $4|36$ e $6|36$ mas $24 \nmid 36$.

$36 = 2^2 \times 3^2$ logo, facilmente se vê que, $4 = 2^2$ e $6 = 2 \times 3$ dividem 36. Mas ao multiplicarmos 4 por 6 estamos a aumentar a potência do factor primo 2 e por isso o produto destes dois números já não divide 36.

Com a apresentação do Lema de Euclides podemos finalmente concluir a demonstração do Teorema Fundamental da Aritmética, provando a unicidade da factorização.

dem (continuação TFA):

Unicidade

Vamos assumir que existe pelo menos um número natural n que tem duas factorizações distintas.

$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_r$, com p_i e q_j , $1 \leq i \leq k, 1 \leq j \leq r$, números primos.

Suponhamos, sem perda de generalidade, que $k \leq r$. Pela igualdade apresentada sabemos que $p_1 | q_1 q_2 \dots q_r$, logo pelo Lema de Euclides $p_1 | q_j$, $1 \leq j \leq r$. Consideremos, por exemplo, que $p_1 | q_1$ (a menos de uma renomeação dos q's. Mas, q_1 é primo e por isso os seus únicos divisores são 1 e q_1. Como p_1, também, é primo temos que $p_1 \neq 1$ e, portanto, $p_1 = q_1$.

Assim, simplificando a igualdade anterior podemos escrever

$$p_2 \dots p_k = q_2 \dots q_r$$

Iterando o processo, iremos obter $p_2 = q_2$, $p_3 = q_3$, …, $p_k = q_k$, a menos de uma reordenação dos q's.

Simplificando de novo a igualdade, como $k < r$, obtemos

$$1 = q_{k+1} \dots q_r$$

Esta igualdade é impossível, logo $k = r$. ■

Número de Divisores

Consideremos, dado $n \in \mathbb{N}$, o conjunto definido por pelos divisores de n. O número de elementos deste conjunto denota-se por $\tau(n)$.

Assim, $\tau(n)$ representa o número de divisores de n.

$$\tau(n) = \#\{d \in \mathbb{N} : d | n\}$$

Para todo $n \in \mathbb{N}$, podemos escrever

$$\tau(n) = \sum_{d|n} 1$$

Por exemplo, se $n = 20$ então $\tau(n) = \#\{1, 2, 4, 5, 10, 20\} = 6$.

Observação.

1. $\tau(n) = 1 \Leftrightarrow n = 1$

2. $\tau(n) = 2 \Leftrightarrow n$ é *primo*

Pela propriedade 10 da divisibilidade verificamos que

$$\{d \in \mathbb{N} : d | n\} = \left\{\frac{n}{d} \in \mathbb{N} : d | n\right\}.$$

Se $n = 12$, por exemplo, temos que $\{1, 2, 3, 4, 6, 12\} = \left\{\frac{12}{1}, \frac{12}{2}, \frac{12}{3}, \frac{12}{4}, \frac{12}{6}, \frac{12}{12}\right\}$.

Problema 2.9. Escolhendo ao acaso um divisor positivo de 10^{99}qual a probabilidade deste ser múltiplo de 10^{88}.

Resolução:

Comecemos por escrever a factorização 10^{99} e 10^{88}. Temos que $10 = 2 \times 5$, logo

$$10^{99} = (2 \times 5)^{99} = 2^{99} \times 5^{99} \text{ e } 10^{88} = (2 \times 5)^{88} = 2^{88} \times 5^{88}$$

Assim, qualquer que seja $d \geq 0$ divisor de 10^{99}, $d = 2^a \times 5^b$ com $0 \leq a, b \leq 99$. Quantos divisores tem 10^{99}? Pela desigualdade apresentada, para cada expoente, a e b, existem 100 hipóteses, logo 10^{99} tem 100^2 divisores (casos possíveis).

Quantos destes divisores são múltiplos de 10^{88}? Para d ser múltiplo de 10^{88}, d tem de ser maior ou igual a 10^{88}, então $88 \leq a, b \leq 99$. Isto é, para cada para cada expoente, a e b, existem 12 hipóteses, logo existem 12^2 divisores de 10^{99} que também são múltiplos de 10^{88} (casos possíveis).

Portanto, a probabilidade pedida é dada pela fracção $\frac{12^2}{100^2} = \frac{9}{625}$.

A resolução do problema do último exemplo poderia ter sido simplificada caso já tivesse sido apresentado o seguinte resultado:

Se $n = {p_1}^{k_1} \ldots {p_r}^{k_r}$ é uma factorização de n, então

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

Usando a igualdade anterior, rapidamente teríamos determinado o número de divisores de $10^{99} = 2^{99} \times 5^{99}$, calculando o produto $(99 + 1)(99 + 1)$.

Problema 2.10. Determina o número de pares ordenados (a, b), com a e b naturais, tal que $\text{mmc}(a, b) = 2^3 \cdot 5^7 \cdot 11^{13}$.

Resolução:

Como $\text{mmc}(a, b) = 2^3 \cdot 5^7 \cdot 11^{13}$ então $a = 2^x \cdot 5^y \cdot 11^z$ e $b = 2^s \cdot 5^t \cdot 11^u$ com $x, y, z, s, t, u \in \mathbb{N}_0$.

Por isso, $3 = \max(x, s)$, $7 = \max(y, t)$ e $13 = \max(z, u)$. Assim, por exemplo, para os valores de x e s, sabemos que um deles tem de ser igual a 3, podendo o outro tomar qualquer valor inteiro entre 0 e 3, isto é, (x, s) pode ser igual $(0, 3)$, $(1, 3)$, $(2, 3)$, $(3, 3)$, $(3, 0)$, $(3, 1)$, $(2, 3)$. Logo, existem 7 hipóteses para (x, s). Analogamente, existem 15 hipóteses para (y, t) e 27 hipóteses para (z, u).

Portanto, há $7 \times 15 \times 27 = 2835$ pares ordenados de números naturais (a, b) cujo mínimo múltiplo comum é igual a $2^3 \cdot 5^7 \cdot 11^{13}$.

O raciocínio utilizado na resolução deste exemplo é idêntico ao aplicado na demonstração do resultado que nos permite dizer que:

Se $n = {p_1}^{k_1} \dots {p_r}^{k_r}$ é uma factorização de n, então existem

$$(2k_1 + 1)(2k_2 + 1) \cdots (2k_r + 1)$$

pares ordenados de números naturais (a, b) com $\text{mmc}(a, b) = n$.

Para finalizar este conteúdo, temos, ainda, uma igualdade que nos permite calcular o produto dos divisores positivos de um número natural.

Para todo $n \in \mathbb{N}$, temos

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

dem:

$$\left(\prod_{d|n} d\right)^2 = \left(\prod_{d|n} d\right) \cdot \left(\prod_{d|n} d\right) = \left(\prod_{d|n} d\right) \cdot \left(\prod_{d|n} \frac{n}{d}\right)$$

$$= \prod_{d|n} d \cdot \frac{n}{d} = \prod_{d|n} n = \underbrace{n \times \dots \times n}_{\tau(n)} = n^{\tau(n)}$$

Este produto tem tantas parcelas quanto o número de divisores de n

Assim, obtemos

$$\underbrace{\left(\prod_{d|n} d\right)^2}_{\geq 0} = \underbrace{n^{\tau(n)}}_{\geq 0} \Leftrightarrow \prod_{d|n} d = \sqrt{n^{\tau(n)}} = n^{\frac{\tau(n)}{2}}$$ ■

Soma dos Divisores

Para todo $n \in \mathbb{N}$ a soma de todos os divisores naturais de n é dada por

$$\sigma(n) = \sum_{d|n} d$$

Observação.

1. $\sigma(n) = 1 \Leftrightarrow n = 1$

2. $\sigma(n) = n + 1 \Leftrightarrow n$ é $primo$

Por exemplo, se $n = 20$ então $\sigma(20) = 1 + 2 + 4 + 5 + 10 + 20 = 42$.

Se $n = {p_1}^{k_1} \ldots {p_r}^{k_r}$ é uma factorização de n, então

$$\sigma(n) = \frac{{p_1}^{k_1+1} - 1}{p_1 - 1} \ldots \frac{{p_r}^{k_r+1} - 1}{p_r - 1}$$

Assim, para o exemplo anterior, como $20 = 2^2 \times 5$ temos

$$\sigma(20) = \frac{2^{2+1} - 1}{2 - 1} \times \frac{5^{1+1} - 1}{5 - 1} = 7 \times 6 = 42$$

dem:

Os divisores de n são da forma

$${p_1}^{a_1} \ldots {p_r}^{a_r}, \text{ com } 0 \leq a_i \leq k_i, i = 1, \ldots, r.$$

Cada divisor de n aparece exactamente uma única vez como parcela na seguinte soma, uma vez aplicada a propriedade distributiva:

$$\underbrace{(1 + p_1 + \ldots + {p_1}^{k_1})}_{\frac{{p_1}^{k_1+1}-1}{p_1-1}} \cdots \underbrace{(1 + p_r + \ldots + {p_r}^{k_r})}_{\frac{{p_r}^{k_r+1}-1}{p_r-1}}$$

Como cada um destes factores representa a soma de uma progressão geométrica de razão $p_i, i = 1, \ldots, k$, obtemos o resultado pretendido. ■

Problema 2.11. Determina soma dos divisores pares de 100 000.

Resolução:

Como $100\,000 = 10^5 = 2^5 \times 10^5$ todos os seus divisores são da forma $2^a \times 10^b$, com $0 \leq a, b \leq 5$. Mas os divisores pares têm de incluir, pelo menos, um 2 na sua factorização, logo são da forma $2^a \times 10^b$ com $1 \leq a \leq 5$ e $0 \leq b \leq 5$.

Assim, a soma dos divisores pares será dada por:

$$(2 \cdot 10^0 + \cdots + 2 \cdot 10^5) + (2^2 \cdot 10^0 + \cdots + 2^2 \cdot 10^5) + \ldots + (2^5 \cdot 10^0 + \cdots + 2^5 \cdot 10^5) =$$

$$= 2(10^0 + \cdots + 10^5) + 2^2(10^0 + \cdots + 10^5) + \cdots + 2^5(10^0 + \cdots + 10^5)$$

$$= \underbrace{(2 + 2^2 + 2^3 + 2^4 + 2^5)}_{\frac{2^{5+1}-1}{2-1}-1} \underbrace{(1 + 10 + 10^2 + 10^3 + 10^4 + 10^5)}_{\frac{5^{5+1}-1}{5-1}}$$

$$= 62 \cdot \frac{5^{5+1} - 1}{5 - 1} = 242\,172$$

Com isto terminamos a teoria relativamente aos problemas que não necessitam de técnicas especiais. De facto, de uma maneira ou de outra, os alunos até ao Ensino Secundário estão familiarizados com os temas estudados até aqui, facilitando o trabalho.

Segue-se um pequeno conjunto de problemas de modo a possibilitar a aplicação dos conteúdos abordados e assim treinar os raciocínios expostos. Serão apresentadas algumas resoluções ou apenas sugestões de resolução.

2.1. Mais alguns problemas

Problema 2.12. Dados dois números primos diferentes, p e q, descobre quantos divisores diferentes tem o número:

a) pq **b)** p^2q **c)** p^2q^2 **d)** p^nq^m

Resolução:

Para qualquer uma das alíneas sabemos qualquer divisor de cada um destes números é da forma $d = p^iq^j$, com i,j inteiros positivos, variando apenas o intervalo de números inteiros a que pertencem os expoentes i e j.

a) Para este caso, mesmo sem utilizar a igualdade anterior, é fácil verificar que os divisores de pq são: $1, p, q$ e pq. Assim, são 4 os divisores de pq.

b) Seja $d = p^iq^j$, d divide p^2q se $0 \leq i \leq 2$ e $0 \leq j \leq 1$. Logo, para o par (i,j) pode ser igual a: $(0,0), (0,1), (1,0), (1,1), (2,0)$ e $(2,1)$; obtendo os divisores $1, q, p, pq, p^2$ e p^2q. Assim, são 6 os divisores de p^2q.

c) Analogamente ao que foi feito para **b)**, temos que $d = p^iq^j$ divide p^2q^2 se $0 \leq i \leq 2$ e $0 \leq j \leq 2$. Então, existem 3 possibilidades para cada um dos expoentes i e j. Portanto, o número de divisores será igual ao número de combinações possíveis entre os expoentes i e j, ou seja, para cada i existem 3 possibilidades para j. Logo, existem $3 \times 3 = 9$ divisores de p^2q^2.

d) É óbvio que a resolução desta questão é análoga às resoluções anteriores, pois trata-se da generalização dos casos estudados.

Escrevendo por outras palavras, cada divisor de $x = p^nq^m$ é igual ao produto entre um divisor p^n e um divisor de q^m, isto é, os divisores de x são as diferentes combinações possíveis entre os divisores de cada um dos primos que compõe x.

Assim, para cada divisor de p^n $(1, p, p^2, \dots, p^n,$ ou seja, $n+1$ divisores) escolhemos um divisor de q^m $(1, q, q^2, \dots, q^n,$ ou seja, $m+1$ divisores). Logo, existem $(n+1)(m+1)$ divisores de p^nq^m.

Utilizando a fórmula para o número de divisores de um número obteríamos rapidamente a resposta.

$$n = {p_1}^{k_1} \dots {p_r}^{k_r}, \qquad \tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

Logo, $\tau(p^n q^m) = (n + 1)(m + 1)$.

Problema 2.13.

a) Prova que o produto de quaisquer três números naturais consecutivos é divisível por 6.

b) Mostra em que condições o produto de quaisquer três números naturais consecutivos é divisível por 12.

Resolução:

a) Para a resolução deste problema há que observar que em qualquer grupo de três números naturais consecutivos existe sempre um número par e existe sempre um número múltiplo de 3. Assim, na factorização deste produto irá constar pelo menos um 2 e um 3. Logo, como a factorização de 6 é igual a 2×3, concluímos que este produto é divisível por 6.

b) Primeiro observemos que $12 = 2^2 \times 3$. Como já vimos, em qualquer grupo de três números consecutivos, um deles é múltiplo de 3, logo na factorização do produto quaisquer três números naturais consecutivos existe pelo menos um factor 3. Assim, para este produto ser divisível por 12, a sua factorização terá de incluir, também, a potência 2^2.

Seja $P = n(n + 1)(n + 2)$, com n natural, o produto de três números naturais consecutivos.

Se n for par então $n + 2$ também é par. Logo, na factorização deste produto irá constar pelo menos dois factores iguais a 2. Assim, produto $2^2 \times 3 = 12$ consta da factorização de P e, portanto, $12|P$.

Se n for ímpar então $n + 1$ é par e $n + 2$ é ímpar. Como o produto de dois números ímpares é ímpar, significa que, para garantirmos a existência da potência 2^2 no produto P, $n + 1$ tem de ser múltiplo de 4.

c) Prova que o produto de quaisquer cinco números naturais consecutivos é divisível por 30.

Sugestão: raciocínio semelhante ao aplicado na alínea **2.1.**

Problema 2.14. Seja n um número natural maior do que 1. Prova que 2^n é a soma de dois números ímpares consecutivos.

Resolução:

Sejam $2k - 1$ e $2k + 1$ dois números impares consecutivos. Então,

$$2k - 1 + 2k + 1 = 4k = 2^2 k$$

Logo, para $k = \underbrace{2^{n-2}}_{\substack{\in \mathbb{Z} \\ \text{porque} \\ n \geq 2}}$ obtemos $2^2 k = 2^2 \cdot 2^{n-2} = 2^n$.

Problema 2.15. Encontra todos os naturais n para os quais as expressões $3n-4$, $4n-5$ e $5n-3$ representam números primos.

Resolução:

Como $3n-4+4n-5+5n-3 = 12n-12$ sabemos que a soma destes três números primos é par, pois $12n-12 = 2(6n+6)$. Assim, no mínimo um destes três números é par, pois a soma de três números ímpares é impar. A soma de dois números é par se ambos forem pares ou se ambos forem ímpares. $4n-5$ não pode ser par pois $4n$ é sempre par para todo o n e 5 é ímpar, logo destes três números, apenas as expressões $3n-4$ e $5n-3$ podem representar números pares.

O único número primo par é o 2, então $3n-4=2$ ou $5n-3=2$.

Se $3n-4=2 \Leftrightarrow n=2$ então $4n-5=3$ e $5n-3=7$.

Se $5n-3=2 \Leftrightarrow n=1$ então $3n-4=-1$ e $4n-5=-1$.

Logo, apenas para $n=2$ as expressões dadas representam números primos.

Problema 2.16. Determina o produto de todos os divisores inteiros positivos distintos de $n = 420^4$.

Resolução:

Na resolução deste problema iremos aplicar a fórmula do produto dos divisores de um número natural, demonstrada no tema Número de divisores:

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

Precisamos de calcular o número de divisores de n, $\tau(n)$, e por isso comecemos por determinar a factorização de n:

$$420^4 = (2^2 \times 3 \times 5 \times 7)^4 = 2^8 \times 3^4 \times 5^4 \times 7^4$$

Assim,

$$\tau(n) = (8+1)(4+1)(4+1)(4+1) = 1125$$

Logo,

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}} = (420^4)^{\frac{1125}{2}} = 420^{2250}$$

Problema 2.17.

a) O Emanuel multiplicou dois números positivos de dois algarismos no seu caderno. Depois substituiu todos os algarismos por letras (algarismos diferentes correspondem a letras diferentes e algarismos iguais correspondem a letras iguais).

No final obteve $\mathrm{AB} \times \mathrm{CD} = \mathrm{EEFF}$. Prova que o Emanuel cometeu um erro.

b) O Emanuel calculou o quadrado de um número positivo de dois algarismos no seu caderno obtendo de novo o número EEFF. Determina os valores de E e de F.

Resolução:

a) Comecemos por analisar o membro da direita da igualdade.

$$\mathrm{EEFF} = \mathrm{EE} \times 10^2 + \mathrm{FF} = (\mathrm{E} \times 10 + \mathrm{E}) \times 10^2 + (\mathrm{F} \times 10 + \mathrm{F})$$
$$= \mathrm{E}(10+1) \times 10^2 + \mathrm{F}(10+1) = 11\mathrm{E} \times 10^2 + 11\mathrm{F} = 11(\mathrm{E} \times 10^2 + \mathrm{F})$$

Verificamos que o número EEFF é divisível por 11. Assim, para a igualdade dada ser verdadeira, também $\mathrm{AB} \times \mathrm{CD}$ terá de ser divisível por 11.

Como 11 é primo, se $11|\mathrm{AB} \times \mathrm{CD}$ então 11 tem de fazer parte da factorização de AB ou de CD, isto é, ou $11|\mathrm{AB}$ ou $11|\mathrm{CD}$. Mas, qualquer número de dois algarismos divisível por 11 o algarismo das dezenas é igual ao algarismo das unidades. Logo, como $\mathrm{A} \neq \mathrm{B}$ e $\mathrm{C} \neq \mathrm{D}$ temos que $11 \nmid \mathrm{AB}$ nem $11 \nmid \mathrm{CD}$.

Portanto, se 11 não divide os dois membros da igualdade significa que $\mathrm{AB} \times \mathrm{CD} \neq \mathrm{EEFF}$ e por isso o Emanuel cometeu um erro.

b) O número obtido é um quadrado perfeito, logo existe n inteiro tal que $\mathrm{EEFF} = n^2$.

Pela alínea anterior, sabemos que EEFF é múltiplo de 11 e, consequentemente, n^2 também é múltiplo de 11. Como n é um número positivo de dois algarismos podemos escrever $n = \mathrm{AA} > 0$. Experimentando os nove casos possíveis (11, 22, 33, 44, 55, 66, 77, 88 e 99) o único número que ao quadro é da forma EEFF é o 88, pois $88^2 = 7744$. Portanto, $\mathrm{E} = 7$ e $\mathrm{F} = 4$.

Problema 2.18. Considera um número escrito com cem algarismos iguais a 0, cem algarismos iguais a 1 e cem algarismos iguais a 2. Poderá este número ser um quadrado perfeito?

Sugestão: Mostra que este número é divisível por 3 mas não é divisível por 9.

Resolução:

Seguindo a sugestão dada, utilizaremos os critérios de divisibilidade por 3 e por 9. Um número é divisível por 3 e por 9 se a soma dos seus algarismos for divisível por 3 e por 9, respetivamente.

Seja n o número em questão, então

$$n = \underbrace{22\ldots22}_{100}\underbrace{11\ldots11}_{100}\underbrace{00\ldots00}_{100}$$

Logo, a soma dos algarismos de n é dada por

$$\underbrace{2+\cdots+2}_{100}+\underbrace{1+\cdots+1}_{100}+\underbrace{0+\cdots+0}_{100}=2\times100+1\times100+0\times100=300$$

Assim, n é divisível por 3 pois $3|300$ mas não é divisível por 9 porque $9 \nmid 300$.

Suponhamos que n é um quadrado perfeito, então $n=({p_1}^{k_1}\ldots\ {p_r}^{k_r})^2$. Como 3 é primo e $3|n$ então existe $1\leq t\leq r$ tal que $p_t=3$. Consideremos, sem perda de generalidade, $p_1=3$, obtemos $n=(3^{k_1}\ldots\ {p_r}^{k_r})^2$, logo $9|n$. Chegamos, assim, a uma contradição e por isso n não pode ser um quadrado perfeito.

Problema 2.19. Qual o último algarismo do número 2^{50}.

Resolução:

As primeiras potências de base 2 são: $2, 4, 8, 16, 32, \ldots$

É fácil perceber que o algarismo das unidades da próxima potência será igual ao produto do algarismo das unidades da potência anterior por 2, ou seja, 4, e assim sucessivamente. Logo, obtemos um ciclo: o último algarismo de 2^5 é igual a 2 como 2^1, o último algarismo de 2^6 é igual a 4 como 2^2, o último algarismo de 2^7 é igual a 8 como 2^3, o último algarismo de 2^8 é igual a 6 como 2^4, etc.

Logo, o algarismo das unidades de uma potência de base 2 repete-se de 4 em 4 potências e por isso é possível determinar o último algarismo de 2^{50}calculando o resto da divisão de 50 por 4.

Como $50=4\times12+2$ então $\underbrace{2^{4\times12}}_{\substack{12\ \text{ciclos}\\ \text{completos}}}\times2$. Logo, o último algarismo de 2^{50}será igual ao segundo elemento do ciclo, coincidindo com o último digito de 2^2, que é igual a 4.

Problema 2.20. Determina o menor número natural n tal que $990|n!$.

Resolução:

Sabemos que $n!$ é o produto de todos os naturais menores ou iguais a n.

$$n!=1\cdot2\cdots(n-1)n$$

Como $990=2\times3^2\times5\times11$ e $990|n!$ então $11|n!$. Assim, 11 tem de dividir o produto $n!$, mas 11 é primo, o que significa que 11 é um dos factores de $n!$ e, portanto, $n\geq11$. Logo, o menor valor de n nas condições do enunciado é $n=11$.

Problema 2.21. Determina $\mathrm{mdc}(111\ldots111, 11\ldots11)$, em que existem cem algarismos 1 na representação decimal do primeiro número e sessenta algarismos 1 na representação decimal do segundo número.

Resolução:

$\underbrace{111\ldots111}_{\text{cem } 1's} = 1\times10^{99}+1\times10^{98}+\cdots+1\times10+1$

$\underbrace{11\ldots11}_{\text{sessenta } 1's} = 1\times10^{59}+1\times10^{58}+\cdots+1\times10+1$

Aplicando o algoritmo de Euclides:

$$\begin{array}{l|l} 1\times10^{99}+\cdots+1\times10^{40}+\cdots+1\times10+1 & 1\times10^{59}+\cdots+1\times10+1 \\ -(1\times10^{99}+\cdots+1\times10^{40}) & \hline 1\times10^{40} \\ \hline 1\times10^{39}+\cdots+1\times10+1 & \end{array}$$

$$\begin{array}{l|l} 1\times10^{59}+\cdots+1\times10^{20}+\cdots+1\times10+1 & 1\times10^{39}+\cdots+1\times10+1 \\ -(1\times10^{59}+\cdots+1\times10^{20}) & \hline 1\times10^{20} \\ \hline 1\times10^{19}+\cdots+1\times10+1 & \end{array}$$

$$\begin{array}{l|l} 1\times10^{39}+\cdots+1\times10^{20}+\cdots+1\times10+1 & 1\times10^{19}+\cdots+1\times10+1 \\ -(1\times10^{39}+\cdots+1\times10^{20}) & \hline 1\times10^{20} \\ \hline 1\times10^{19}+\cdots+1\times10+1 & \end{array}$$

$$\begin{array}{l|l} 1\times10^{19}+\cdots+1\times10+1 & 1\times10^{19}+\cdots+1\times10+1 \\ -(1\times10^{19}+\cdots+1\times10+1) & \hline 1 \\ \hline 0 & \end{array}$$

Logo, $\text{mdc}(111\ldots111, 11\ldots11) = \underbrace{1\times10^{19}+\cdots+1\times10+1}_{\text{vinte } 1's}$

Problema 2.22. Qual o maior número natural n para o qual n^3+100 é divisível por $n+10$.

Resolução:

Façamos a divisão de n^3+100 por $n+10$ utilizando, por exemplo, a regra de Ruffini.

	1	0	0	100
-10		-10	100	-1000
	1	-10	100	-900

Então,

$$n^3 + 100 = (n + 10)(n^2 - 10n + 100) - 900$$

Como $n + 10$ divide $n^3 + 100$ e $(n + 10)(n^2 - 10n + 100)$ então $n + 10$ também divide 900.

O maior divisor de 900 é o próprio 900, logo o maior valor que $n + 10$ pode tomar é 900. Portanto, o maior valor que n pode tomar é 890.

Problema 2.23. Seja n um inteiro maior do que 2. Mostra que, de entre as fracções,

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

existe um número par de frações irredutíveis.

Resolução:

Para a resolução deste problema é necessário observar que $\text{mdc}(a, b) = \text{mdc}(a - b, b)$, isto é, $d|a$ e $d|b \Leftrightarrow d|a - b$ e $d|b$. Esta equivalência é facilmente demonstrada utilizando as propriedades 7 e 8 da divisibilidade.

Assim, a fracção $\frac{k}{n}$ é irredutível se e só se a fracção $\frac{n-k}{n}$ é irredutível, pois $\text{mdc}(k, n) = \text{mdc}(n - k, n)$.

Se $\frac{k}{n} \neq \frac{n-k}{n}$ para todo k, então emparelhando-as obtemos um número par de fracções irredutíveis.

Se $\frac{k}{n} = \frac{n-k}{n}$, para algum k, então $n = 2k$. Logo, a fracção é redutível pois $\frac{k}{n} = \frac{k}{2k} = \frac{1}{2}$ e por isso o problema reduz-se ao caso anterior.

Problema 2.24. Sejam $a, b \in \mathbb{N}$ tais que $\text{mmc}(a, b) + \text{mdc}(a, b) = a + b$. Prova que um dos dois números é divisível pelo outro.

Resolução:

Queremos provar que ou $a|b$ ou $b|a$.

Sejam $d = \text{mdc}(a, b)$ e $m = \text{mdc}(a, b)$.

Como $d|a$ e $d|b$ podemos escrever $a = dt$ e $b = ds$, $t, s \in \mathbb{N}$.

Visto que $\frac{a}{d}$ e $\frac{b}{d}$ são coprimos, a partir da relação entre o mdc e o mmc, temos

$$\text{mdc}(a, b) \times \text{mmc}(a, b) = ab \Leftrightarrow dm = ab \Leftrightarrow m = \frac{ab}{d} \Leftrightarrow m = tsd$$

Assim, podemos escrever a igualdade do enunciado da seguinte forma:

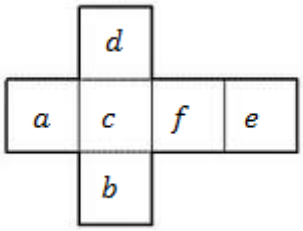
$$\text{mmc}(a,b) + \text{mdc}(a,b) = a + b \Leftrightarrow tsd + d = dt + ds \underbrace{\Leftrightarrow}_{d>0}$$
$$\Leftrightarrow ts + 1 = t + s$$
$$\Leftrightarrow ts - t - s + 1 = 0$$
$$\Leftrightarrow (t-1)(s-1) = 0$$
$$\Leftrightarrow t = 1 \vee s = 1$$

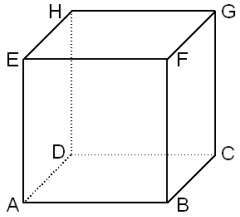
Se $t = 1$, então $a = t$, logo $b = ds = as$, ou seja, $a|b$. Se $s = 1$, então $b = d$, logo $a = dt = bt$, ou seja, $b|a$.

Problema 2.25. Um número natural é escrito em cada face de um cubo. A cada vértice é atribuído o produto dos números escritos nas três faces que intersectam o vértice. A soma dos números atribuídos a cada vértice é igual a 1001. Descobre a soma dos número escritos nas faces do cubo.

Resolução:

Sejam a, b, c, d, e e f os números escritos em cada uma das faces, com a e f, b e d, c e e escritos em faces opostas, e A, B, C, D, E e F os vértices do cubo. Suponhamos que na face ABF está escrito o número c.





Então, $A = abc$; $B = bcf$; $C = bef$; $D = abe$; $E = acd$; $F = cdf$; $G = def$ e $H = ade$.

Assim,

$$1001 = abc + bcf + bef + abe + acd + cdf + def + ade =$$
$$= abc + +abe + acd + ade + bcf + bef + cdf + def$$
$$= ab(c+e) + ad(c+e) + bf(c+e) + df(c+e)$$
$$= (c+e)(ab + ad + bf + df)$$
$$= (c+e)[a(b+d) + f(b+d)]$$
$$= (c+e)(a+f)(b+d)$$

Como $1001 = 7 \times 11 \times 13$ e cada uma das somas $c+e, a+f$ e $b+d$ é maior do que 1 então $\{c+e, a+f, b+d\} = \{7, 11, 13\}$. Logo,

$$a + b + c + d + e + f = 7 + 11 + 13 = 31$$

Problema 2.26. Dizemos que um número composto que não é divisível por 2, 3 ou 5 tem "aspecto de primo". Por exemplo, os números 49, 77 e 91 são os menores nestas condições. Sabendo que existem 168 números primos menores do que 1000, quantos números menores do que 1000 têm "aspecto de primo"?

Resolução:

Para facilitar a resolução deste problema vamos definir $n = \lfloor x \rfloor$ como o maior inteiro menor ou igual a x.

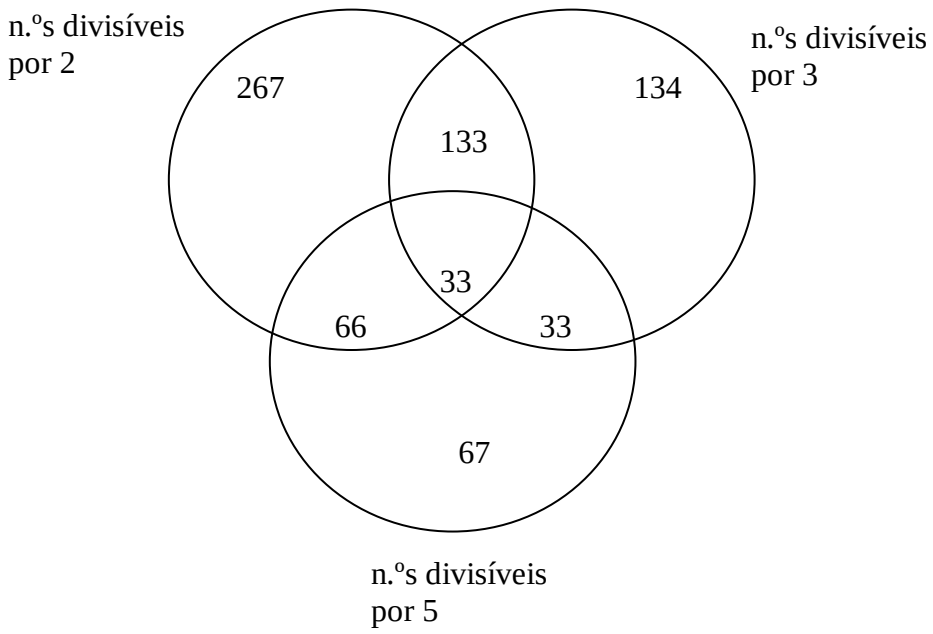
Existem 999 números menores do que 1000. Destes 999 números, $\left\lfloor \frac{999}{2} \right\rfloor = 499$ são pares, ou seja, divisíveis por 2; $\left\lfloor \frac{999}{3} \right\rfloor = 333$ são divisíveis por 3 e $\left\lfloor \frac{999}{5} \right\rfloor = 199$ são divisíveis por 5.

Mas existem números que são simultaneamente divisíveis por mais do que um destes números. Assim, interessa-nos saber quantos números são divisíveis por 6, 10, 15 e 30.

Temos que, há $\left\lfloor \frac{999}{6} \right\rfloor = 166$ números divisíveis por 6; $\left\lfloor \frac{999}{10} \right\rfloor = 99$ divisíveis por 10; $\left\lfloor \frac{999}{15} \right\rfloor = 66$ divisíveis por 15 e $\left\lfloor \frac{999}{30} \right\rfloor = 33$ divisíveis por 30.

Portanto, existem $499 + 333 + 199 - 166 - 99 - 66 + 33 = 733$ números que são divisíveis por pelo menos um dos números 2, 3 e 5.

Para facilitar vejamos o seguinte diagrama de Venn:



Confirmamos que existem $733 = 267 + 134 + 67 + 66 + 133 + 33 + 33$ números que são divisíveis por pelo menos um dos números 2, 3 e 5.

Dos restantes $999 - 733 = 266$ números, 165 são primos diferentes de 2, 3 ou 5. Como, o número 1 não é primo nem composto, temos $266 - 165 - 1 = 100$ números com "aspecto de primo".

Problema 2.27. O número $27\,000\,001$ tem exactamente quatro factores primos. Determina a sua soma.

Resolução:

Vejamos que $300^3 = 27\,000\,000$, logo podemos escrever

$$27\,000\,001 = 27\,000\,000 + 1 = 300^3 + 1$$

Como $\underbrace{x^3 + 1}_{\downarrow} = (x+1)(x^2 - x + 1)$ e $x^2 - y^2 = (x+y)(x-y)$, temos que

Facilmente se vê que -1 é uma raiz deste polinómio e obtemos a factorização apresentada

$$\begin{aligned} 27\,000\,001 = 300^3 + 1 &= (300+1)(300^2 - 300 + 1) = \\ &= 301(\underbrace{300^2 + 2 \times 300 + 1}_{(300+1)^2} - 900) \\ &= 301[(300+1)^2 - 900]) = 301(301^2 - 30^2) \\ &= 301(301+30)(301-30) = 301 \times \underbrace{331}_{\text{primo}} \times \underbrace{271}_{\text{primo}} \\ &= 7 \times 43 \times 271 \times 331 \end{aligned}$$

Portanto, a resposta é $7 + 43 + 271 + 331 = 652$.

Problema 2.28. Mostra que $n! + 1$ e $(n+1)! + 1$ são coprimos.

Resolução:

$n! + 1$ e $(n+1)! + 1$ são coprimos se e só se $\text{mdc}(n! + 1, (n+1)! + 1) = 1$

$$\begin{array}{l|l} (n+1)! + 1 & n! + 1 \\ \hline -(n+1)! - n - 1 & n + 1 \\ \hline -n & \end{array} \qquad \begin{array}{l|l} n! + 1 & -n \\ \hline (-n)! & -(n-1)! \\ \hline 1 & \end{array} \qquad \begin{array}{l|l} -n & 1 \\ \hline n & -n \\ \hline 0 & \end{array}$$

Portanto, $\text{mdc}(n! + 1, (n+1)! + 1) = \text{mdc}(n! + 1, -n) = \text{mdc}(-n, 1) = 1$.

Problema 2.29. Encontra vinte números compostos e consecutivos.

Resolução:

Por exemplo, a sequência $20! + 2, 20! + 3, \ldots, 20! + 21$ satisfaz as condições do enunciado.

Vejamos que

$21! + 2 = 21 \times 20 \times \ldots \times 2 + 2 = 2 \times (21 \times 20 \times \ldots \times 3 + 1)$, logo $2|21! + 2$

$21! + 3 = 21 \times 19 \times \ldots \times 3 \times 2 + 3 = 3 \times (21 \times 20 \times \ldots \times 4 \times 2 + 1)$, logo $3|21! + 3$

$\vdots$

$21! + 21 = 21 \times 20 \times \ldots \times 3 \times 2 + 21 = 21 \times (20 \times \ldots \times 2 + 1)$, logo $21|21! + 21$

Do exemplo, facilmente se percebe que para qualquer n natural, a sequência $n! + k$ com $2 \leq k \leq n$, é formada por $n - 1$ números compostos e consecutivos.

3. Teoremas úteis

Neste capítulo, pretende-se expor um conjunto de resultados que permitirão resolver problemas mais complexos, que exigem um maior aprofundamento na teoria dos números. Os teoremas mais importantes serão demonstrados com a principal finalidade de apresentar raciocínios e estratégias que serão úteis para descobrir a solução de alguns problemas.

Ao contrário dos temas estudados no capítulo anterior, a teoria aqui apresentada não é trabalhada no ensino não superior. No entanto, por utilizar muitos dos resultados anteriores é possível torná-la acessível aos alunos mais interessados.

Equações Diofantinas

No capítulo 2 foi apresentada a Identidade de Bézout que diz que se $d = \text{mdc}(a, b)$, então existem inteiros x, y tais que $d = ax + by$. Iremos agora estudar um pouco sobre estas equações.

A equações do tipo $c = ax + by$ chamam-se equações diofantinas lineares a duas variáveis. Esta designação deve-se ao matemático grego Diofanto (século III d. C.), autor do livro *Aritmética*, que se dedicou à resolução de equações em $\mathbb{Z}$ e em $\mathbb{Q}$. A todas as equações para as quais procuramos soluções inteiras ou racionais chamamos de equações diofantinas, sendo as equações lineares a duas variáveis as mais simples.

Também foi visto na secção anterior que a equação $c = ax + by$ tem solução se e só se $\text{mdc}(a, b)|c$. Por exemplo, a equação $56 = 63x + 14y$ tem solução pois $\text{mdc}(63, 14) = 7$ e $7|56$. Para além disso, vimos como é possível escrever $\text{mdc}(63, 14)$ como combinação linear de 63 e 14.

Neste caso,

$$\begin{aligned} 7 &= 63 + 14 \times (-4) \\ 56 &= 63 \times 8 + 14 \times (-32) \end{aligned} \quad \times 8, \text{ pois } 56 = 7 \times 8$$

Logo, $(8, -32)$ é uma solução desta equação, mas não é a única.

Proposição. Sejam a, b e c inteiros e $d = \text{mdc}(a, b)$. Se (x_0, y_0) for uma solução particular de $ax + by = c$, então as restantes soluções são dadas por

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \qquad t \in \mathbb{Z}$$

dem:

Sabemos que a equação $ax + by = c$ tem solução se e só se $d|c$.

Se (x_0, y_0) é uma solução então $ax_0 + by_0 = c$. Seja (x', y') outra solução da equação dada então $ax' + by' = c$. Fazendo a diferença entre as duas equações obtemos

$$\begin{array}{r} ax' + by' = c \\ \underline{ax_0 + by_0 = c} \\ a(x' - x_0) + b(y' - y_0) = 0 \end{array}$$

Ou seja,

$$a(x' - x_0) = -b(y' - y_0) \Leftrightarrow a(x' - x_0) = b(y_0 - y')$$

Façamos $r = \frac{a}{d}$ e $s = \frac{b}{d}$ então pela proposição **3.1.6.** r e s são coprimos.

Dividindo a última equação por d, obtemos

$$r(x' - x_0) = s(y_0 - y')$$

Assim, desta igualdade verificamos que $r|s(y_0 - y')$, mas r e s são coprimos, logo pelo Lema de Euclides $r|(y_0 - y')$, isto é, $y_0 - y' = tr$. Então $y' = y_0 - tr = y_0 - \frac{a}{d}t$.

Substituindo $y_0 - y'$ por tr na equação $r(x' - x_0) = s(y_0 - y')$ obtemos

$r(x' - x_0) = srt \Leftrightarrow (x' - x_0) = st \Leftrightarrow x' - x_0 = \frac{b}{d}t \Leftrightarrow x' = x_0 + \frac{b}{d}t$ ■

Problema 3.1. (Problema das cem aves) Este problema foi enunciado num livro chinês do século V, *Manual aritmético*, de Zhang Quijan.

Um galo compra-se por 5 *qian*, uma galinha por 3 *qian* e 3 pintos por 1 *qian*. Se 100 aves forem compradas por 100 *qian*, quantos galos, galinhas e pintos há?

Resolução:

Sejam x, y, z números naturais.

x - representa o número de galos

y - representa o número de galinhas

z - representa o número de pintos

Traduzindo problema para linguagem matemática, obtemos o seguinte sistema:

$$\begin{cases} x + y + z = 100 \\ 5x + 3y + \frac{1}{3}z = 100 \end{cases}$$

Simplificando,

$$\begin{cases} z = 100 - x - y \\ 5x + 3y + \frac{1}{3}(100 - x - y) = 100 \end{cases} \Leftrightarrow \begin{cases} z = 100 - x - y \\ 5x - \frac{1}{3}x + 3y - \frac{1}{3}y = 100 - \frac{100}{3} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} z = 100 - x - y \\ 14x + 8y = 200 \end{cases} \Leftrightarrow \begin{cases} z = 100 - x - y \\ 7x + 4y = 100 \end{cases}$$

A equação $7x + 4y = 100$ é uma equação Diofantina que tem soluções se e só se $\text{mdc}(7,4)|100$.

Apesar de ser fácil determinar o $\text{mdc}(7,4)$ sem cálculos, iremos fazê-los aplicando o algoritmo de Euclides.

$$\begin{array}{r|l} 7 & 4 \\ \hline 3 & 1 \end{array} \qquad \begin{array}{r|l} 4 & 3 \\ \hline 1 & 1 \end{array} \qquad \begin{array}{r|l} 3 & 1 \\ \hline 0 & 3 \end{array}$$

Como $1|100$ sabemos que a equação tem solução e podemos escrever $1 = \text{mdc}(7,4)$ da seguinte forma:

$$1 = 4 - 3$$
$$1 = 4 - (7 - 4)$$
$$1 = (-1) \times 7 + 2 \times 4$$

Mas, queremos escrever 100 como combinação linear de 7 e 4. Logo multiplicamos ambos os membros da última igualdade por 100, obtendo o pretendido:

$$100 = (-100) \times 7 + 200 \times 4$$

Sendo $(x_0, y_0) = (-100, 200)$ uma solução particular da equação $7x + 4y = 100$ as soluções gerais são dadas por:

$$x = -100 + 4t \text{ e } y = 200 - 7t, t \in \mathbb{Z}$$

Substituindo na primeira equação do sistema, temos

$$z = 100 - x - y = 100 - (-100 + 4t) - (200 + 7t) = 3t$$

Assim,

$$\begin{cases} x + y + z = 100 \\ 5x + 3y + \frac{1}{3}z = 100 \end{cases} \Leftrightarrow \begin{cases} x = -100 + 4t \\ y = 200 + 7t \\ z = 3t \end{cases}$$

No entanto, no contexto do problema, sabemos que $x, y, z > 0$.

$x = -100 + 4t > 0 \Leftrightarrow t > 25$

$y = 200 - 7t > 0 \Leftrightarrow t < \frac{200}{7} = 28 + \frac{4}{7}$

$z = 3t > 0 \Leftrightarrow t > 0$

Portanto, temos que $25 < t < 28 + \frac{4}{7}$, $t \in \mathbb{Z}$, logo t só pode ser igual a 26, 27 ou 28.

Para $t = 26$,

$$x = -100 + 4 \times 26 = 4;\ y = 200 - 4 \times 26 = 18;\ z = 3 \times 26 = 78$$

Para $t = 27$,

$$x = 8;\ y = 11;\ z = 81$$

Para $t = 28$,

$$x = 12;\ y = 4;\ z = 84$$

Congruências

Na resolução de problemas referentes à divisibilidade, muitas vezes, é conveniente trabalhar, não com os números dados, mas com os seus restos quando divididos por um outro número. Assim, outra abordagem às questões relativas à divisibilidade é através dos restos, conhecida como a teoria das congruências. Desenvolvida pelo matemático alemão Gauss (1777-1855) no seu livro *Disquisitiones Arithmeticae* (tradução do latim: Investigações aritméticas).

> *Se um número n mede a diferença entre dois números a e b, então a e b dizem-se congruentes em relação a n; caso contrário, incongruentes.*
>
> Gauss

Definição. Sejam $a, b \in \mathbb{Z}, n \in \mathbb{N}$. Dizemos que a é congruente com b módulo n se $n|(a - b)$. Escreve-se $a \equiv b$.

Observação: Se a não é congruente com b, escreve-se $a \not\equiv b$.

O símbolo utilizado para representar uma congruência também foi introduzido por Gauss, tendo sido escolhido devido às semelhanças da relação de congruência com a relação de igualdade.

É possível explicar esta relação utilizando um conceito presente no nosso dia-a-dia, a medição do tempo. A medição do tempo está relacionada a fenómenos cíclicos, como é o caso dos dias ou dos anos. Em relação ao dia sabemos que de 24 horas em 24 horas o relógio "reinicia" a contagem.

Imaginemos uma situação em que duas pessoas diferentes, A e B, partem às 22h do mesmo dia para uma viagem de 8 e 32 horas, respetivamente.

Logo, não dizemos que a pessoa A chegou às 30h e que a pessoa B chegou às 54h. Na verdade, dizemos que ambas chegaram às 6h. Mas, como é possível?

Se pensarmos apenas no que foi dito até agora, faria sentido escrever

$$22 + 8 = 22 + 32 = 6$$

No entanto, igualdade é falsa e, obviamente, deve-se ao facto de terem chegado em dias diferentes.

Na verdade, temos que $22 + 8 = 30 = 24 + 6$ e $22 + 32 = 54 = 24 \times 2 + 6$. Assim, podemos desprezar os múltiplos de 24, subtraindo-os ou adicionando-os, até obtermos a hora certa.

Portanto, neste caso, dizemos que $32 \equiv 54 \pmod{24}$, isto é,

$$22 + 8 \equiv 22 + 32 \equiv 6 \pmod{24}$$

Proposição. Sejam $a, b \in \mathbb{Z}, n \in \mathbb{N}$. Os números a e b são congruentes módulo n se e só se a e b têm o mesmo resto na divisão por n.

dem:

($\Longrightarrow$)

Da divisão de a por n podemos escrever $a = nq_a + r_a$ e da divisão de b por n podemos escrever $b = nq_b + r_b$, com $q_a, q_b, r_a, r_b \in \mathbb{Z}$.

Logo, podemos escrever

$$\begin{array}{r} a = nq_a + r_a \\ b = nq_b + r_b \\ \hline a - b = n(q_a - q_b) + (r_a - r_b) \end{array}$$

a e b são congruentes módulo n, ou seja, $n|a - b$, e $n|\ n(q_a - q_b)$, logo $n|(r_a - r_b)$.

$$\begin{array}{r} 0 \leq r_a \leq n \\ -n \leq -r_b \leq 0 \\ \hline -n \leq r_a - r_b \leq n \end{array}$$

Como $r_a - r_b$ é múltiplo de n e $-n \leq r_a - r_b \leq n$ então $r_a - r_b = 0$. Portanto, $r_a = r_b$.

($\Longleftarrow$)

Se a e b têm o mesmo resto na divisão por n então podemos escrever $a = nq_a + r$ e $b = nq_b + r$, com $q_a, q_b, r \in \mathbb{Z}$.

Assim,

$$\begin{array}{c} a = nq_a + r \\ b = nq_b + r \\ \hline a - b = n(q_a - q_b) \end{array}$$

Logo, $n|a - b$. ■

A próxima proposição é consequência imediata do resultado anterior.

Proposição. A relação de congruência é uma relação de equivalência, isto é:

(a) $a \equiv a \pmod{n}$

(b) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$

(c) Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$

A classe de congruência de um número inteiro a é definida pelo conjunto $\{b \in \mathbb{Z}: b \equiv a\}$.

Cada resto possível na divisão por n dá origem a uma classe de congruência.

Por exemplo, se $n = 4$, temos quatro classes de congruência. A figura a seguir exemplifica as classes módulo 4.

Legenda:

Classe do zero ■ Classe do 1■ Classe do 2■ Classe do 3■

Proposição. Sejam $a, b, a', b' \in \mathbb{Z}$, $n \in \mathbb{N}$. Se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, então:

$$a + b \equiv a' + b' \pmod{n} \quad \text{e} \quad ab \equiv a'b' \pmod{n}$$

Em particular, $c \in \mathbb{Z}$, $k \in \mathbb{N}$

- $a + c \equiv a' + c \pmod{n}$
- $ac \equiv a'c \pmod{n}$
- $a^k \equiv (a')^k \pmod{n}$

dem:

Iremos demonstrar apenas para o produto, $ab \equiv a'b' \pmod{n}$, deixando as restantes para praticar.

$a \equiv a' \pmod{n}$ então $a - a' = tn \Leftrightarrow a = a' + tn$

$b \equiv b' \pmod{n}$ então $b - b' = sn \Leftrightarrow b = a' + sn$

Logo,

$ab = (a' + tn)(a' + sn) = a'b' + tb'n + a'sn + tsn^2 = a'b' + n\underbrace{(tb' + a's + ts)}_{\in \mathbb{Z}}$

Portanto, $ab = a'b' + rn \Leftrightarrow ab - a' = rn, r \in \mathbb{Z}$, ou seja, $ab \equiv a'b' (\text{mod } n)$. ■

Observação:

Seja r o resto da divisão de a por n então $a \equiv r$, pois $a = qn + r \Leftrightarrow a - r = qn$.

Problema 3.2. Mostra que $n^5 + 4n$ é divisível por 5, para todo n inteiro.

Resolução:

Este problema é idêntico ao problema 2. Mas, agora, iremos resolvê-lo aplicando as congruências. Iremos analisar os possíveis restos da divisão de n por 5, ou seja, iremos trabalhar com o módulo 5.

Se $n \equiv 0$ então $n^5 \equiv 0$ e $4n \equiv 0$, logo $n^5 + 4n \equiv 0 \pmod 5$

Se $n \equiv 1$ então $n^5 \equiv 1^5 = 1$ e $4n \equiv 4$, logo $n^5 + 4n \equiv 5 \equiv 0 \pmod 5$

Se $n \equiv 2$ então $n^5 \equiv 2^5 = 32$ e $4n \equiv 8$, logo $n^5 + 4n \equiv 40 \equiv 0 \pmod 5$

Se $n \equiv 3$ então $n^5 \equiv 3^5 = 243$ e $4n \equiv 12$, logo $n^5 + 4n \equiv 255 \equiv 0 \pmod 5$

Se $n \equiv 4$ então $n^5 \equiv 4^5 = 1024$ e $4n \equiv 16$, logo $n^5 + 4n \equiv 1040 \equiv 0 \pmod 5$

Problema 3.3. Prova que $30^{99} + 61^{100}$ é divisível por 31.

Resolução:

$30 \equiv -1$ então $30^{99} \equiv -1 \pmod{31}$

$61 \equiv -1$ então $61^{100} \equiv 1 \pmod{31}$

Logo, $30^{99} + 61^{100} \equiv -1 + 1 = 0 \pmod{31}$.

Problema 3.4. Qual o resto da divisão do número $10^{10} + 10^{100} + 10^{1000} + 10^{10000} + + \cdots + 10^{10000000000}$ por 7?

Resolução:

Como $10 \equiv 3$ então $10^{10} \equiv 3^{10} = (3^5)^2 = 243^2 \pmod 7$

$243 = 34 \times 7 + 5$, logo $243^2 \equiv 5^2 = 25 \equiv 4 \pmod 7$

Assim, temos

$10^{100} = (10^{10})^{10} \equiv 4^{10} = (4^5)^2 = 1024^2 \equiv 2^2 = 4 \pmod 7$

$\downarrow$

$1024 = 146 \times 7 + 2$

$$10^{1000} = (10^{100})^{10} \equiv 4^{10} \equiv 4 \pmod 7$$

$$\vdots$$

$$10^{10000000000} \equiv 4 \pmod 7$$

Logo,

$$10^{10} + 10^{100} + 10^{1000} + 10^{10000} + + \cdots + 10^{10000000000} \equiv 4 \times 10 = 40 \equiv 5 (\text{mod } 7)$$

Os famosos critérios de divisibilidade, estudados no Ensino Básico, são um bom exemplo da aplicabilidade das congruências. Vejamos como podemos utilizar as congruências para "descobrir" o critério de divisibilidade por 9.

Seja $n \in \mathbb{N}$, como podemos determinar o resto da divisão de n por 9?

É conhecida dos alunos a representação de um número na base 10, em que qualquer número natural se escreve de maneira única na forma

$$n = a_t \times 10^t + a_{t-1} \times 10^{t-1} + \cdots + a_1 \times 10 + a_0$$

Com $a_k \in \{0, 1, 2, 3, \ldots, 9\}$, $0 \leq k \leq t$ e $a_t \neq 0$.

Iremos usar a congruência módulo 9. Como $10 \equiv 1$ pois $10 - 1 = 9 \equiv 0 (\text{mod } 9)$ então $10^t \equiv 1^t = 1 \pmod 9$.

Logo,

$$\begin{aligned} n &= a_t \times 10^t + a_{t-1} \times 10^{t-1} + \cdots + a_1 \times 10 + a_0 \\ &\equiv a_t \times 1 + a_{t-1} \times 1 + \cdots + a_1 \times 1 + a_0 \\ &\equiv a_t + a_{t-1} + \cdots + a_1 + a_0 \end{aligned}$$

Portanto, o resto na divisão de n por 9 é igual ao resto da divisão da soma dos seus algarismos por 9.

Por exemplo, $9 \nmid 3427$ porque o resto da divisão de 3427 por 9 é diferente de zero.

$$3 + 4 + 2 + 7 = 16 \equiv 7 \pmod 9$$

Isto é, n é divisível por 9 se e só se a soma dos seus algarismos for divisível por 9.

Com o mesmo raciocínio obtemos o critério de divisibilidade por 3 pois, também, $10 \equiv 1 \pmod 3$.

Desta forma, facilmente se deduzem os restantes critérios de divisibilidade.

Existem muitas outras áreas com aplicações práticas das congruências, como por exemplo a prova dos nove, o ISBN (*International Standard Book Number*) ou o número do bilhete de identidade.

Proposição (Regras de cálculo). Sejam $a, b \in \mathbb{Z}, n \in \mathbb{N}$.

1. Se $c|a, b, n$ então $a \equiv b(\mathrm{mod}\, n) \Leftrightarrow \frac{a}{c} \equiv \frac{b}{c} \left(\mathrm{mod}\, \frac{n}{c}\right)$

2. Se $ca \equiv cb \pmod{n}$, então $a \equiv b \left(\mathrm{mod}\, \frac{n}{d}\right)$ em que $d = \mathrm{mdc}(c, n)$.

Em particular, se $ca \equiv cb \pmod{n}$ com c e n coprimos, então $a \equiv b \pmod{n}$.

3. Se $ca \equiv cb \pmod{p}$ com p primo e $p \nmid c$, então $a \equiv b \pmod{p}$.

dem:

1. $a \equiv b(\mathrm{mod}\, n) \Leftrightarrow n|a - b$. Então,

$\frac{a-b}{n} \in \mathbb{Z} \Leftrightarrow \frac{\frac{a}{c} - \frac{b}{c}}{\frac{n}{c}} \in \mathbb{Z} \Leftrightarrow \frac{a}{c} \equiv \frac{b}{c} \left(\mathrm{mod}\, \frac{n}{c}\right)$

2. $ca \equiv cb \pmod{n} \Leftrightarrow n|ca - cb$. Então, $ca - cb = c(a - b) = kn$.

Se $d = \mathrm{mdc}(c, n)$ então $\frac{c}{d}$ e $\frac{n}{d}$ são coprimos.

Dividindo a igualdade $c(a - b) = kn$ por d obtemos,

$$\underbrace{\frac{c}{d}}_{s}(a - b) = k\underbrace{\frac{n}{d}}_{r}$$

$r|s(a - b)$, mas r e s são coprimos, logo $r|(a - b)$, isto é, $a \equiv b \left(\mathrm{mod}\, r = \frac{n}{d}\right)$.

3. Sai da demonstração de **2.**, pois neste caso $d = 1$.

4. Sai da demonstração de **2.**, pois se p é primo e $p \nmid c$, entãp p e c são coprimos. ■

Equações Lineares com Congruências

É possível considerar equações com congruências e neste trabalho serão abordadas mas mais simples, que são da forma $ax \equiv b \pmod{n}$ com $a, b \in \mathbb{Z}, n \in \mathbb{N}$.

Começamos por observar que se a equação $ax \equiv b \pmod{n}$ tiver solução, então tem infinitas soluções. Isto é, se x for solução da equação e $x' \equiv x \pmod{n}$, então x' também é uma solução

$$ax' \equiv ax \equiv b \pmod{n}$$

Por exemplo, consideremos a equação $2x \equiv 4 \pmod{6}$. Como estamos a trabalhar com módulo 6, sabemos que x será congruente com um dos restos possíveis da divisão por 6: 0, 1, 2, 3, 4 ou 5.

Experimentando cada um dos valores possíveis verificamos que apenas 2 e 5 são soluções da equação.

$$2 \times 2 = 4 \equiv 4 \text{ e } 2 \times 5 = 10 \equiv 4 \pmod{6}$$

Assim, todos os elementos da classe de congruência do 2 e da classe do 5 são soluções da equação.

Classe do $2 = \{\dots, -10, -4, 2, 8, 14, \dots\}$; Classe do $5 = \{\dots, -7, -1, 5, 11, 17, \dots\}$

$$2 \times (-10) = -20 \equiv 4 \text{ e } 2 \times 11 = 22 \equiv 4 \pmod 6$$

No entanto, nem sempre é viável experimentar um elemento de cada classe, ou pelo menos não o faríamos caso estivemos a trabalhar com módulo 100…

Proposição. A equação $ax \equiv b \pmod n$ tem solução se e só se $d = \text{mdc}(a, n) | b$. Neste caso, há d soluções não congruentes, duas a duas.

Verificamos que,

$$ax \equiv b \pmod n \Leftrightarrow \underbrace{ax + ny = b}_{\text{Equação diofantina}}$$

Em geral as soluções desta equação são da forma

$$x = x_0 + \frac{n}{d}t$$

Observação: Existem *d* soluções diferentes.

Corolário. Se $\text{mdc}(a, n) = 1$ (em particular, se n for primo e não dividir a), então a equação tem uma e uma só solução (módulo n).

Proposição. Seja $d = \text{mdc}(a, n)$, a equação $ax \equiv b \pmod n$ pode ser simplificada para

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod } \frac{n}{d}\right)$$

Exemplos: Vejamos dois exemplos de como resolver equações lineares.

1. $6x \equiv 3 \pmod{15}$

A equação tem solução pois $3 = \text{mdc}(6, 15) | 3$, e existem 3 soluções módulo 15.

Simplificando,

$$2x \equiv 1 \pmod 5$$

Como o módulo é pequeno podemos experimentar os 5 valores possíveis e determinar uma solução particular da equação. De facto, neste caso, como $1 = \text{mdc}(2,5)$, sabemos que esta equação tem apenas uma solução módulo 5:

$$2 \times 0 = 0 \not\equiv 1 \quad 2 \times 1 = 2 \not\equiv 1 \quad 2 \times 2 = 4 \not\equiv 1 \quad \underbrace{2 \times 3 = 6 \equiv 1}_{\substack{3 \text{ é uma solução} \\ \text{particular}}} \quad 2 \times 4 = 8 \not\equiv 1$$

Logo, as três soluções da são:

$$3 + \underbrace{\frac{15}{3}}_{5} \times 0 = 3 \; ; \quad 3 + \frac{15}{3} \times 1 = 8 \quad \text{e} \quad 3 + \frac{15}{3} \times 2 = 13$$

Assim, todos os números congruentes com 3, 8 ou 13 são também soluções da equação. Portanto, as soluções gerais são da forma:

$$3 + 15t \; ; 8 + 15t \text{ e } 13 + 15t$$

2. $25x \equiv 15 \pmod{29}$

A equação tem solução pois $1 = \text{mdc}(25,29) | 15$, e existe apenas 1 solução módulo 29.

Neste exemplo, não é praticável experimentar todas as possibilidades por isso iremos aplicar o método geral.

$$25x \equiv 15 \pmod{29} \Leftrightarrow \underbrace{25x + 29y = 15}_{\text{Equação diofantina}}$$

Utilizando algoritmo de Euclides podemos determinar x e y tal que $1 = 25x + 29y$.

$$\begin{array}{r|l} 29 & 25 \\ \hline 4 & 1 \end{array} \qquad \begin{array}{r|l} 25 & 4 \\ \hline 1 & 6 \end{array} \qquad \begin{array}{r|l} 4 & 1 \\ \hline 0 & 4 \end{array}$$

$$\begin{aligned} 1 &= 25 - 4 \times 6 \\ 1 &= 25 - (29 - 25 \times 1) \times 6 \\ 1 &= 25 - (29 \times 6 - 25 \times 6) \\ 1 &= 25 \times 7 + 29 \times (-6) \end{aligned}$$

Logo,

$$15 = 25 \times \underbrace{105}_{x} + 29 \times (-90)$$

Já vimos que a equação tem apenas uma solução e é $x = \underbrace{105}_{29 \times 3 + 18} \equiv 18 \pmod{29}$.

Portanto, as soluções gerais são da forma $x = 18 + 29t$.

Teorema chinês dos restos

Iremos agora considerar sistemas de congruências. A resolução destes sistemas baseia-se num método que aparece pela primeira vez na resolução de um problema do século III, que abordaremos de seguida. Falamos do famoso Teorema chinês dos restos.

Teorema chinês dos restos. Sejam $n_1, \dots, n_r$ coprimos dois a dois, e $, \dots, a_r \in \mathbb{Z}$. Então o sistema de congruências

$$x \equiv a_1 \pmod{n_1} \qquad x \equiv a_2 \pmod{n_2} \qquad x \equiv a_r \pmod{n_r}$$

tem solução única, módulo $n_1 \cdots n_r$.

dem:

Seja $N = n_1 \cdots n_r$, para $1 \leq k \leq r$ definimos $N_k = \frac{N}{n_k} = n_1 \cdots n_{k-1} n_{k-1} \cdots n_r$.

Consideremos a equação $N_k x \equiv 1 (\mathrm{mod}\, n_k)$. Como os números n_k são coprimos dois a dois então N_k é coprimo com n_k, logo a equação $N_k x \equiv 1 (\mathrm{mod}\, n_k)$ tem solução módulo n_k. Seja x_k essa solução.

Então, a solução do sistema ai ser dada por

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

Seja $1 \leq k \leq r$, verifiquemos que $\bar{x}$ é solução de $x \equiv a_k \pmod{n_k}$. Observemos que, se $t \neq k$ então $a_t N_t x_t \equiv 0 \pmod{n_k}$, pois neste caso N_t contém o factor n_k. Além disso, $N_k x_k \equiv 1 (\mathrm{mod}\, n_k)$ por definição de x_k.

Assim,

$$\bar{x} = \underbrace{a_1 N_1 x_1}_{\equiv 0} + \underbrace{a_2 N_2 x_2}_{\equiv 0} + \cdots + a_k \underbrace{N_k x_k}_{\equiv 1} + \cdots + \underbrace{a_r N_r x_r}_{\equiv 0} \equiv a_k \pmod{n_k}$$

Se x' for outra solução, então $\forall k$

$$x' \equiv a_k \equiv \bar{x} \pmod{n_k} \Leftrightarrow n_k | x - x'$$

Como os números n_k são coprimos dois a dois então $N = n_1 \cdots n_r | (x' - \bar{x}) \pmod{N}$. ■

Problema 3.5. (Problema de Sun-Tzu)

Temos coisas, das quais não conhecemos o número.

Dividida por 3, o resto é 2,

por 5, o resto é 3,

e por 7 o resto é 2.

Qual será o número?

Resolução:

Simplificando, pretende-se encontrar um número com restos 2, 3 e 2 na divisão por 3, 5 e 7, respectivamente.

Para resolver este problema temos de considerar o seguinte sistema de equações

$$x \equiv 2 \pmod{3} \quad x \equiv 3 \pmod{5} \quad x \equiv 2 \pmod{7}$$

Consideremos $N = 3 \times 5 \times 7$, logo $N_1 = 35$, $N_2 = 21$ e $N_3 = 15$.

Pelo Teorema chinês dos restos, temos de resolver as seguintes equações

$35x \equiv 1 \underbrace{\Leftrightarrow}_{35 \equiv 2} 2x \equiv 1 (\mathrm{mod}\ 3)$	$21x \equiv 1 \underbrace{\Leftrightarrow}_{21 \equiv 1} x \equiv 1 (\mathrm{mod}\ 5)$	$15x \equiv 1 \underbrace{\Leftrightarrow}_{15 \equiv 1} x \equiv 1 (\mathrm{mod}\ 7)$
Por tentativas, obtemos $2 \times 2 = 4 \equiv 1\ (\mathrm{mod}\ 3)$ Logo, $x_1 = 2$	Logo, $x_2 = 1$ $\times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$ $33\ (\mathrm{mod}\ \underbrace{105}_{3 \times 5 \times 7})$	Logo, $x_3 = 1$

A solução geral do sistema é dado por $x = 233 + 105t$. Estas soluções podem ser também dadas por $\underbrace{23}_{233 - 105 \times 2} + 105t$.

Pequeno Teorema de Fermat e Teorema de Euler

Definição. Seja $n \in \mathbb{N}$. Dizemos que $\{a_1, \dots, a_n\}$ é um sistema completo de resíduos se $a_i \not\equiv a_j\ (\mathrm{mod}\ n)$ se $i \neq j$.

Observação. Sejam $a \in \mathbb{Z}$ e $\{a_1, \dots, a_n\}$ um sistema completo de resíduos, então $a \equiv a_i$ para um e um só i.

Proposição: Seja $\{a_1, \dots, a_n\}$ um sistema completo de resíduos $\mathrm{mod}\ n$ e a coprimo com n, então $\{aa_1, \dots, aa_n\}$ é também um sistema completo de resíduos.

Por exemplo, $\{0, 1, 2, 3\}$ e $\{4, 5, 6, 7\}$ são dois sistemas completos de resíduos (s.c.r) módulo 4. Mas, também, $\underbrace{\{3, 6, 9, 12\}}_{\text{múltiplos de 3}}$ é um s.c.r, mas $\underbrace{\{2, 4, 6, 8\}}_{\text{múltiplos de 2}}$ já não é um s.c.r. pois 2 e 4 não são coprimos.

Pequeno Teorema de Fermat. Se p primo, então

$$a^{p-1} \equiv 1\ (\mathrm{mod}\ p) \text{ se } p \nmid a,$$
$$a^p \equiv a\ (\mathrm{mod}\ p) \text{ para todo } a \in \mathbb{Z}.$$

dem:

Seja p primo, $p \nmid a$

$\{0, 1, 2, \dots, p-1\}$ é um s.c.r. Pela proposição anterior $\{0, a, 2a, \dots, (p-1)a\}$ também é um s.c.r.

Assim, podemos escrever,

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv a \times 2a \times 3a \times \cdots \times (p-1)a\ (\mathrm{mod}\ p)$$

Logo, $(p-1)! \equiv (p-1)!\, a^{p-1}$. Como todos os números que aparecem são coprimos com p podemos simplificar a equação, obtendo $1 \equiv a^{p-1} \pmod{p}$.

Suponhamos agora que a é qualquer. Se a for coprimo com p, então $1 \equiv a^{p-1}$ e $a \equiv a^p$. Se não for, $a \equiv 0 \equiv 0^p \equiv a^p \pmod{p}$. ■

Problema 3.6. Qual o resto da divisão de 3^{102} por 101.

Resolução:

Pretendemos descobrir b tal que $3^{102} \equiv b \pmod{101}$.

Como 101 é primo e $101 \nmid 3$, pelo pequemo teorema de Fermat sabemos que $3^{100} \equiv 1$.

Assim, $3^{102} = 3^{100} \cdot 3^2 \equiv 3^{100} \cdot 9 \equiv 9 \pmod{101}$.

Problema 3.7. Prova que $300^{3000} - 1$ é divisível por 1001.

Resolução:

Factorizando o número 1001, obtemos $1001 = 7 \times 11 \times 13$.

Vejamos então quais os restos da divisão de 300^{3000} por 7, 11 e 13.

Como 7, 11 e 13 são primos temos que

$$300^6 \equiv 1 \pmod{7},\ 300^{10} \equiv 1 \pmod{11} \text{ e } 300^{12} \equiv 1 \pmod{13}.$$

Logo,

$$300^{500\times 6} = (300^6)^{500} \equiv 1^6 = 1 \pmod{7}$$
$$300^{300\times 10} = (300^{10})^{300} \equiv 1^{10} = 1 \pmod{11}$$
$$300^{250\times 12} = (300^{12})^{250} \equiv 1^{12} = 1 \pmod{13}$$

Portanto, $300^{3000} \equiv 1 \pmod{7, 11, 13}$, isto é, $300^{3000} - 1$ é divisível por 7, por 11 e por 13. Logo, $7 \times 11 \times 13 = 1001 | 300^{3000} - 1$.

Definição (Função de Euler). Seja $n \in \mathbb{N}$. A função φ conta o número de elementos que há entre 1 e n, coprimos com n; isto é,

$$\varphi(n) = \#\{m: 1 \leq m \leq n \text{ e } \mathrm{mdc}(m,n) = 1\}$$

A tabela que se segue apresenta os primeiros valores de $\varphi(n)$.

n	coprimos com n	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4

Proposição. Se p primo então

$$\varphi(n) = p - 1 \text{ e } \varphi(n) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Teorema de Euler. Se a coprimo com $n \in \mathbb{N}$, então

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Este teorema também é conhecido como o Grande Teorema de Fermat.

Teorema: Se m e n coprimos $\varphi(mn) = \varphi(m)\varphi(n)$.

Problema 3.8. Mostra que $n^{37} - n$ é divisível por 1729.

Resolução:

Comecemos por calcular a factorização de 1729.

$$1729 = 7 \times 13 \times 19$$

Então, $1729 | n^{37} - n$ se e só se $7 \times 13 \times 19 | n^{37} - n$, isto é, se e só se cada um dos factores dividir $n^{37} - n$.

$n^{37} = (n^6)^6 \cdot n$ mas $n^6 \equiv 1 \pmod 7$ logo $(n^6)^6 \cdot n \equiv 1^6 \cdot n = n$
$n^{37} = (n^{12})^3 \cdot n$ mas $n^{12} \equiv 1 \pmod{13}$ logo $(n^{12})^3 \cdot n \equiv 1^3 \cdot n = n$
$n^{37} = (n^{18})^2 \cdot n$ mas $n^{18} \equiv 1 \pmod{19}$ logo $(n^{18})^2 \cdot n \equiv 1^2 \cdot n = n$

Portanto, $7, 13, 19 | n^{37} - n$, isto é, $1729 = 7 \times 13 \times 19 | n^{37} - n$.

4. Problemas avançados

Vejamos agora alguns problemas onde podem ser aplicados os conteúdos estudados no capítulo anterior.

Problema 4.1. (Mahaviracarya, 850) Havia 63 pilhas de fruta e 7 frutos soltos. Os frutos foram divididos por 23 viajantes. Qual o número de frutos em casa pilha.

Resolução:

Sejam x, y números naturais em que

x – representa o n.º de frutos por pilha

y – representa o n.º de frutos de cada viajante

O problema pode ser traduzido pela seguinte equação

$$63x + 7 = 23y \Leftrightarrow$$
$$\Leftrightarrow -63x + 23y = 7$$

$$\begin{array}{r|l} -63 & 23 \\ \hline 6 & -3 \end{array} \qquad \begin{array}{r|l} 23 & 6 \\ \hline 5 & 3 \end{array} \qquad \begin{array}{r|l} 6 & 5 \\ \hline 1 & 1 \end{array} \qquad \begin{array}{r|l} 5 & 1 \\ \hline 0 & 5 \end{array}$$

A equação tem solução pois $\text{mdc}(63, 23) = 1 | 7$.

$1 = 6 - 5 \times 1$

$1 = 6 - (23 - 6 \times 3)$ ← $5 = 23 - 6 \times 3$

$1 = 6 - 23 + 6 \times 3$

$1 = 6 \times 4 - 23$

$1 = (-63 - 23 \times (-3)) \times 4 - 23$ ← $6 = -63 - 23 \times (-3)$

$1 = -63 \times 4 + 23 \times 12 - 23$

$1 = -63 \times 4 + 23 \times 11$

$7 = -63 \times \underbrace{28}_{x_0} + 23 \times \underbrace{77}_{y_0}$

Então, $x = 28 + 23t$ e $y = 77 + 63t$.

Como $x, y > 0$ temos $t > -\frac{28}{23} \wedge t > -\frac{77}{63}$.

Logo, para todo inteiro $t \geq -1$, $x = 28 + 23t$ é solução do problema.

Problema 4.2. Reduz 6^{100} módulo 7.

Resolução:

Como $6 - 1 = 7$ temos que $6 \equiv -1 \pmod 7$.

Logo, $6^{100} \equiv (-1)^{100} = 1 \pmod 7$.

Problema 4.3. Mostra que $43^{101} + 23^{101}$ é divisível por 66.

Resolução:

Como $66 = 2 \times 3 \times 11$, sabemos que $43^{101} + 23^{101}$ é divisível por 66 se e só se $2, 3, 11 | 43^{101} + 23^{101}$.

Como $43 = 2 \times 21 + 1 \equiv 1 \pmod 2$ então $43^{101} \equiv 1^{101} = 1 \pmod 2$.

Como $23 = 2 \times 11 + 1 \equiv 1 \equiv 1 \pmod 2$ então $23^{101} \equiv 1^{101} = 1 \pmod 2$.

Logo, $43^{101} + 23^{101} \equiv 1 + 1 = 2 \equiv 0 \pmod 2$, isto é, $2 | 43^{101} + 23^{101}$.

Como $43 = 3 \times 14 + 1 \equiv 1 \pmod 3$ então $43^{101} \equiv 1^{101} = 1 \pmod 3$.

Como $23 = 3 \times 7 + 2 \equiv 2 \equiv -1 \pmod 3$ então $23^{101} \equiv (-1)^{101} = -1 \pmod 3$.

Logo, $43^{101} + 23^{101} \equiv 1 + (-1) = 0 \pmod 3$, isto é, $3 | 43^{101} + 23^{101}$.

Como $43 = 11 \times 3 + 10 \equiv 10 \equiv -1 \pmod{11}$ então $43^{101} \equiv (-1)^{101} = -1 \pmod{11}$.

Como $23 = 11 \times 2 + 1 \equiv 1 \pmod{11}$ então $23^{101} \equiv 1^{101} = 1 \pmod{11}$.

Logo, $43^{101} + 23^{101} \equiv -1 + 1 = 0 \pmod{11}$, isto é, $11 | 43^{101} + 23^{101}$.

Portanto, $2 \times 3 \times 11 = 66 | 43^{101} + 23^{101}$.

Problema 4.4. Encontra três inteiros consecutivos, sendo cada um divisível por um quadrado perfeito.

Sugestão: encontrar a tal que $2^2 | a$, $3^2 | a + 1$ e $5^2 | a + 2$.

Resolução:

Seguindo a sugestão, pretende-se um número a tal que

$$2^2 | a \Leftrightarrow a \equiv 0 \pmod{2^2}$$
$$3^2 | a + 1 \Leftrightarrow a + 1 \equiv 0 \Leftrightarrow a \equiv -1 \equiv 8 \pmod{3^2}$$
$$5^2 | a + 2 \Leftrightarrow a + 2 \equiv 0 \Leftrightarrow a \equiv -2 \pmod{5^2}$$

Assim, obtemos um sistema de congruências com três equações,

$$a \equiv 0 \pmod 4 \qquad a \equiv 8 \pmod 9 \qquad a \equiv -2 \pmod{25}$$

Iremos utilizar o Teorema chinês dos restos para resolver este sistema.

Consideremos $N = 4 \times 9 \times 25$, logo $N_1 = 9 \times 25 = 225$, $N_2 = 4 \times 25 = 100$ e $N_3 = 4 \times 9 = 36$.

Assim, temos de resolver as seguintes equações auxiliares

$225x \equiv 1 \underbrace{\Leftrightarrow}_{225 \equiv 1} x \equiv 1 (\text{mod } 4)$

Logo, $x_1 = 1$

$100x \equiv 1 \underbrace{\Leftrightarrow}_{100 \equiv 1} x \equiv 1 (\text{mod } 9)$

Logo, $x_2 = 1$

$36x \equiv 1 \underbrace{\Leftrightarrow}_{36 \equiv 11} 11x \equiv 1 (\text{mod } 25)$

Podemos determinar x_3 por tentativas ou resolvendo a equação diofantina $11x + 25(-y) = 1$.

Façamos um cálculo auxiliar para determinar x_3:

Como $\text{mdc}(11, 25) = 1$, utilizando o algoritmo de Euclides podemos escrever

$$1 = 3 - 2$$
$$1 = 3 - (11 - 3 \times 3)$$
$$1 = 3 \times (-4) - 11$$
$$1 = (25 - 11 \times 2) \times 4 - 11$$
$$1 = 25 \times 4 + 11 \times (-9)$$

Logo, $x_3 = -9$.

Portanto, uma solução do sistema será dada por

$$a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 0 \times 225 \times 1 + 8 \times 100 \times 1 + (-2) \times 36 \times (-9)$$
$$= 1448 \ (\text{mod } \underbrace{900}_{4 \times 9 \times 25})$$

A solução geral do sistema é dado por $x = 1448 + 105t$. Estas soluções podem ser também dadas por $x = \underbrace{548}_{1448 - 900} + 900t$.

Portanto, por exemplo, os números 548, 549 e 550 são uma solução do problema.

Verifica-se que, de facto, $2^2 | 548$, $3^2 | 549$ e $5^2 | 550$.

Problema 4.5. Existe algum número natural n tal que $n^2 + n + 1$ é divisível por 1955?

Resolução:

Factorizando 1955, obtemos

$$1955 = 5 \times 17 \times 23$$

Assim, $n^2 + n + 1 \equiv 0 \pmod{1955}$ se e só se $n^2 + n + 1 \equiv 0 \pmod{5, 17, 23}$.

Comecemos por investigar se $5 | n^2 + n + 1$.

Se $n \equiv 0$ então $n^2 + n + 1 \equiv 1 \pmod 5$.

Se $n \equiv 1$ então $n^2 + n + 1 \equiv 3 \pmod 5$.

Se $n \equiv 2$ então $n^2 + n + 1 \equiv 7 \equiv 2 \pmod 5$.

Se $n \equiv 3$ então $n^2 + n + 1 \equiv 13 \equiv 3 \pmod 5$.

Se $n \equiv 4$ então $n^2 + n + 1 \equiv 21 \equiv 1 \pmod 5$.

Logo, $n^2 + n + 1 \not\equiv 0 \pmod 5$, para todo n natural. Portanto, se $n^2 + n + 1$ não é divisível por 5, então também não é divisível por 1955.

Problema 4.6. Quantos números de quatro algarismos, com os algarismos do meio iguais a 97 são divisíveis por 45?

Resolução:

Seja $a97b$ a representação decimal do referido número de quatro algarismos.

Como $45 = 9 \times 5$, sabemos que $9, 5 | a97b$. Pelos critérios de divisíbilidade de 9 e de 5 temos que b só pode tomar os valores: 0 ou 5; e $a + 9 + 7 + b \equiv 0 \pmod 9$.

Se $b = 0$ então $a + 9 + 7 + b \equiv 0 \Leftrightarrow a + 16 \equiv 0 \Leftrightarrow a \equiv 2 \pmod 9$.

Se $b = 5$ então $a + 9 + 7 + b \equiv 0 \Leftrightarrow a + 21 \equiv 0 \Leftrightarrow a \equiv 6 \pmod 9$.

Portanto, existem apenas dois números nas condições do enunciado: 2970 e 6975.

Problema 4.7. Seja n um inteiro. Prova que:

a) $n^2 \equiv 0$ ou $1 \pmod 3$.

b) $n^2 \equiv 0$ ou $\pm 1 \pmod 5$.

c) $n^2 \equiv 0$ ou 1 ou $4 \pmod 8$.

d) $n^3 \equiv 0$ ou $\pm 1 \pmod 9$.

e) $n^4 \equiv 0$ ou $1 \pmod{16}$.

Resolução:

A verificação destes casos será útil para a resolução de outros problemas. Sendo o raciocínio análogo em todas as alíneas, apenas algumas serão resolvidas.

a) Em módulo 3 temos que $n \equiv 0, 1$ ou 2. Analisemos os três casos possíveis:

Se $n \equiv 0$ então $n^2 \equiv 0$.
Se $n \equiv 1$ então $n^2 \equiv 1^2 \equiv 1$.
Se $n \equiv 2$ então $n^2 \equiv 2^2 = 4 \equiv 1$.

Logo, $n^2 \equiv 0$ ou $1 \pmod 3$, como queriamos provar.

b) Em módulo 5 temos que $n \equiv 0, 1, 2, 3$ ou 4. Analisemos todos os casos possíveis:

Se $n \equiv 0$ então $n^2 \equiv 0$.
Se $n \equiv 1$ então $n^2 \equiv 1^2 \equiv 1$.
Se $n \equiv 2$ então $n^2 \equiv 2^2 = 4 \equiv -1$.
Se $n \equiv 3$ então $n^2 \equiv 3^2 = 9 \equiv 4 \equiv -1$.
Se $n \equiv 4$ então $n^2 \equiv 4^2 = 16 \equiv 1$.

Logo, $n^2 \equiv 0$ ou $\pm 1 \pmod 5$, como queriamos provar.

d) Em módulo 9 temos que $n \equiv 0, 1, 2, 3, 4, 5, 6, 7$ ou 8. Analisemos todos os casos possíveis:

Se $n \equiv 0$ então $n^3 \equiv 0$
Se $n \equiv 1$ então $n^3 \equiv 1^3 \equiv 1$
Se $n \equiv 2$ então $n^3 \equiv 2^3 = 8 \equiv -1$
Se $n \equiv 3$ então $n^3 \equiv 3^3 = 27 \equiv 0$
Se $n \equiv 4$ então $n^3 \equiv 4^3 = 64 \equiv 1$
Se $n \equiv 5$ então $n^3 \equiv 5^3 = \underbrace{125}_{13\times 9+8} \equiv 8 \equiv -1$
Se $n \equiv 6$ então $n^3 \equiv 6^3 = \underbrace{216}_{24\times 9} \equiv 0$
Se $n \equiv 7$ então $n^3 \equiv 7^3 = \underbrace{343}_{38\times 9+1} \equiv 1$
Se $n \equiv 8$ então $n^3 \equiv 8^3 = \underbrace{512}_{56\times 9+8} \equiv 8 \equiv -1$

Logo, $n^3 \equiv 0$ ou $\pm 1 \pmod 9$, como queriamos provar.

Problema 4.8. Seja k o produto dos primeiros números primos (mais do que um primo). Prova que o número $k-1$ não pode ser um quadrado perfeito.

Resolução:

Pela definição de k sabemos que um dos seus factores é igual a 3, isto é, k é divisível por 3.

Logo, $k-1 \equiv 2 \pmod 3$. Pelo alíena **a)** do problema **4.4.** sabemos que um quadrado perfeito é congruente com 0 ou com 1 em módulo 3. Portanto, $k-1$ não pode ser um quadrado perfeito.

Problema 4.9. Descobre todos os primos p e q tal que $p+q=(p-q)^3$.

Resolução:

Como $p+q=(p-q)^3 \neq 0$, p e q são distintos e por isso coprimos.

Como $p+q \equiv 0 \pmod{p+q}$, temos que

$p+q=-(p+q)=-p-q \equiv 0 \Leftrightarrow -p-q+2p=p-q \equiv 2p \pmod{p+q}$

Assim,

$$p-q \equiv 2p \Leftrightarrow \underbrace{(p-q)^3}_{p+q} \equiv 8p^3 \Leftrightarrow 0 \equiv 8p^3 \pmod{p+q}$$

Mas, p e q são coprimos e por isso também p e $p+q$ são coprimos.

Logo, $0 \equiv 8 \pmod{p+q}$, isto é, $p+q|8$.

Analogamente, $2p \equiv p-q \equiv 0 \pmod{p-q}$. Como p e q são coprimos, também o são p e $p-q \pmod{p-q}$. Logo, $2 \equiv 0$, ou seja, $p-q|2$. Como os divisores de 2 são os números 1 e 2, facilmente se verifica que $p-q=2$ e por isso $p+q=2^3=8$.

Portanto, $p=5$ e $q=2$.

Problema 4.10. Seja p primo. Prova que p divide ab^p-ba^p para todos os inteiros a e b.

Resolução:

Comecemos por observar que $ab(b^{p-1}-a^{p-1})$.

Se $p|ab$ então $p|ab^p-ba^p$. Mas se $p \nmid ab$, então p e a são coprimos, assim como p e b.

Pelo pequeno teorema de Fermat temos que $b^{p-1} \equiv 1$ e $a^{p-1} \equiv 1 \pmod p$, isto é, $b^{p-1} \equiv a^{p-1} \pmod p$. Logo, $b^{p-1}-a^{p-1} \equiv 0 \pmod p$, ou seja, $p|b^{p-1}-a^{p-1}$. Portanto, $p|ab^p-ba^p$ para todo p.

Problema 4.11. Seja p primo com $p > 5$. Prova que $p^8 \equiv 1 \pmod{240}$.

Resolução:

$p^8 \equiv 1 \Leftrightarrow p^8 - 1 \equiv 0 \pmod{240}$, ou seja, se e só se $240|p^8 - 1$. Factorizando, obtemos $240 = 2^4 \times 3 \times 5$. Logo, $240|p^8 - 1$ se e só se $2^4, 3, 5|p^8 - 1$, isto é, se e só se $p^8 \equiv 1 \pmod{2^4, 3, 5}$.

Pelo pequeno teorema de Fermat $p^2 \equiv 1 \pmod{3}$ e $p^4 \equiv 1 \pmod{5}$, pois $p > 5$ e por isso, p é coprimo com 3 e com 5. Assim,

$$p^8 = (p^2)^4 \equiv 1^4 = 1 \pmod{3} \text{ e } p^8 = (p^4)^2 \equiv 1^2 = 1 \pmod{5}$$

Qualquer número ímpar e 2^4 são primos entre si, logo 2^4 e $p > 5$ são coprimos. Pelo teorema de Euler temos que $p^{\varphi(2^4)} \equiv 1$. Como $\varphi(2^4) = 2^4\left(1 - \frac{1}{2}\right) = 2^3$ temos que $p^{\varphi(2^4)} = p^8 \equiv 1 \pmod{2^4}$.

Portanto, $p^8 \equiv 1 \pmod{2^4, 3, 5}$ e, por isso, $p^8 \equiv 1 \pmod{240}$.

Problema 4.12. A soma dos algarismos do número 4444^{4444} na sua representação decimal é igual a A. Seja B a soma dos algarismos de A. Determina a soma dos algarismos de B.

Resolução:

Sejam $a = 4444^{4444}$ e $S(n)$ a soma dos algarismos do número n na sua representação decimal para todo n natural.

Como $4444 < 10000 = 10^4$ podemos escrever $4444^{4444} < (10^4)^{4444} = 10^{17776}$

Logo, a não pode ter mais do que 17776 algarismos na sua representação decimal.

Como cada algarismo é no máximo igual a 9, temos que $A \leq 17776 \times 9 = 159984$.

Dos números naturais menores ou iguais do que 159984, o número com a maior soma dos algarismos que o constituem é o 99999. Por isso, $B \leq 5 \times 9 = 45$. Assim, dos números menores do que 45, o 39 é o número com o maior valor da soma dos seus algarismos. Logo, a soma dos algarismos de $B \leq 12$.

Utilizando o critério de divisibilidade por 9, temos que

$$S(B) \equiv B \equiv S(A) \equiv A \equiv S(a) \equiv a = 4444^{4444} \pmod{9}$$

Portanto, basta saber o resto da divisão de a por 9.

Como $4 + 4 + 4 + 4 = 16 \equiv 7 \equiv -2 \pmod{9}$ temos que

$$4444^{4444} \equiv (-2)^{4444} \equiv (-2)^{3\times 1481+1} \equiv ((-2)^3)^{1481} \times (-2) \equiv$$
$$\equiv \underbrace{(-8)}_{\equiv 1}^{1481} \times (-2) \equiv -2 \equiv 7 \pmod{9}$$

Logo, a soma dos algarismos de B é igual a 7.

Problema 4.13. Seja p um primo da forma $3k+2$ que divide a^2+ab+b^2 para alguns inteiros a e b. Prova que a e b são ambos divisíveis por p.

Resolução:

Iremos resolver este problema tentando chegar a uma contradição, por isso suponhamos que $p \nmid a$.

Como p divide a^2+ab+b^2 e $a^3-b^3=(a-b)(a^2+ab+b^2)$ então também divide a^3-b^3. Logo, $a^3 \equiv b^3 \pmod{p}$.

Assim, podemos escrever $a^{3k} \equiv b^{3k} \pmod{p}$.

Por isso, p também não divide b. Aplicando o pequeno teorema de Fermat vem que $a^{p-1} \equiv 1$ assim como $b^{p-1} \equiv 1 \pmod{p}$, isto é, $a^{p-1} \equiv b^{p-1}$. Logo, como p é da forma $3k+2$ temos que

$$a^{3k+1} \equiv b^{3k+1} \pmod{p}$$

Portanto, $a^{3k} \cdot a \equiv \underbrace{b^{3k}}_{\equiv a^{3k}} \cdot b \equiv a^{3k} \cdot b \pmod{p}$. Como $p \nmid a$, isto é, a e p são coprirmos, então $a \equiv b \pmod{p}$. Esta conclusão e o facto de $a^2 + a\underbrace{b}_{\equiv a} + \underbrace{b}_{\equiv a}^{\,2} \equiv 0 \pmod{p}$ implica que $3a^2 \equiv 0 \pmod{p}$. Como $p = 3k+2 \neq 3$ vem que p divide a, o que contradiz a hipótese.

Problema 4.14. Determina todos os inteiros positivos n para os quais $n!+5$ é um cubo perfeito.

Resolução:

Para a resolução deste problema iremos utilzar o que já foi provado na alínea **d)** do problema **4.4**: qualquer cubo é congruente com 0, 1 ou -1 em módulo 9.

Vejamos o que acontece para os primeiros valores de n.

$n=1, n!+5=6 \equiv 6 \pmod{9}$

$n=2, n!+5=7 \equiv 7 \pmod{9}$

$n=3, n!+5=11 \equiv 2 \pmod{9}$

$n=4, n!+5=29 \equiv 2 \pmod{9}$

$n=5, n!+5=125 \equiv 8 \equiv -1 \pmod{9}$

$n=6, n!+5=725 \equiv 5 \pmod{9}$

Assim, verifica-se que para $1 \leq n \leq 6$ apenas quando $n=5$ a expressão $n!+5$ representa um cubo perfeito.

Quando n toma valores maiores do que 6 temos que $3^2=9$ divide $n!$, isto é, $n! \equiv 0$, pois na factorização de $n!$ constam, pelo menos, dois factores iguais a 3.

Logo, se $n \geq 6$ então $n!+5 \equiv 5 \pmod{9}$.

Portanto, $n!+5$ é um cubo perfeito apenas para $n=5$.

Problema 4.15. Prova que 10^{3n+1} não pode representar a soma de dois cubos perfeitos.

Sugestão: Verifica que qualquer cubo perfeito é congruente com $0, 1$ ou ± 1 módulo 7 .

Resolução:

Vimos que qualquer cubo é congruente com 0, 1 ou -1 em módulo 9. Então por que razão utilizar módulo 7 em vez de módulo 9?

Em módulo 9, a soma de dois cubos é sempre congruente com um dos números: $-2, -1, 0, 1, 2$. Como $10 \equiv 1 \pmod 9$ então $10^{3n+1} \equiv 1^{3n+1} = 1$. No entanto, não podemos concluir nada, pois o recíproco do que foi verificado em **4.4. d)** não é verdadeiro.

Vamos então seguir a sugestão e trabalhar em módulo 7.

Analogamente ao que foi feito em **4.4. d)**, facilmente verificamos que qualquer cubo perfeito é congruente com $0, 1$ ou -1 módulo 7.

Se $n \equiv 0$ então $n^3 \equiv 0$

Se $n \equiv 1$ então $n^3 \equiv 1^3 \equiv 1$

Se $n \equiv 2$ então $n^3 \equiv 2^3 = 8 \equiv 1$

Se $n \equiv 3$ então $n^3 \equiv 3^3 = 27 \equiv 6 \equiv -1$

Se $n \equiv 4$ então $n^3 \equiv 4^3 = 64 \equiv 1$

Se $n \equiv 5$ então $n^3 \equiv 5^3 = \underbrace{125}_{17\times 7+6} \equiv 6 \equiv -1$

Se $n \equiv 6$ então $n^3 \equiv 6^3 = \underbrace{216}_{30\times 7+6} \equiv 6 \equiv -1$

Assim, a soma de dois cubos é sempre congruente com um dos números: $-2, -1, 0, 1, 2 \pmod 7$.

Como $10 \equiv 3 \pmod 7$ então $10^{3n+1} \equiv 3^{3n+1} = (3^3)^n \cdot 3 = 27^n \cdot 3 \equiv (-1)^n \cdot 3 \pmod 7$.

Logo,

se n for par temos $10^{3n+1} \equiv 1 \cdot 3 = 3$

se n for ímpar temos $10^{3n+1} \equiv 1 \cdot 3 = -3$.

Portanto, 10^{3n+1} não pode representar a soma de dois cubos perfeitos.

Problema 4.16. Prova que $11^{n+2}+12^{2n+1}$ é divisível por 133 para qualquer que seja n natural.

Resolução:

$$\begin{aligned}11^{n+2}+12^{2n+1} &= 11^n\cdot 11^2+12^{2n}\cdot 12 = 121\cdot 11^n+12^{2n}\cdot 12\\ &= 11^n(\underbrace{121+12}_{133}-12)+12^{2n}\cdot 12\\ &= \underbrace{133\cdot 11^n}_{\substack{\equiv 0\\ \bmod 133}}-12\cdot 11^n+12\cdot 12^{2n}\\ &\equiv 12(12^{2n}-11^n)\ (\bmod 133)\\ &= 12(\underbrace{144^n}_{\substack{\equiv 11\\ \bmod 133}}-11^n)\equiv 0\ (\bmod 133)\end{aligned}$$

Problema 4.17. Mostra que qualquer número natural é congruente com o seu último algarismo módulo 10, módulo 2 e módulo 5.

Resolução:

Seja n natural. Podemos escrever

$$n = a_t\times 10^t + a_{t-1}\times 10^{t-1}+\cdots+a_1\times 10+a_0$$

Então

$$n-a_0 = a_t\times 10^t + a_{t-1}\times 10^{t-1}+\cdots+a_1\times 10 \equiv 0\ (\bmod 10)$$

Isto é, $n\equiv a_0\ (\bmod 10)$.

Portanto, ao subtrairmos o último algarismo a n obtemos um número cujo algarismo das unidades é igual a zero e por isso divisível por 10.

Como $10=2\times 5$, verificamos que este número também é divisível por 2 e por 5, ou seja,

$$n\equiv a_0(\bmod 10,2,5).$$

Problema 4.18. É possível escrever um quadrado perfeito usando apenas os algarismos 2, 3 e 6, cada um deles, exactamente dez vezes?

Sugestão: utiliza congruências módulo 9.

Resolução:

Seja n um quadrado perfeito nas condições do enunciado.

A soma dos algarismos de é igual a $2\times 10+3\times 10+6\times 10=110\equiv 2\ (\bmod 9)$.

Mas, nenhum quadrado perfeito é congruente com 2 em módulo 9, como podemos verificar:

Se $n \equiv 0$ então $n^2 \equiv 0$

Se $n \equiv 1$ então $n^2 \equiv 1$

Se $n \equiv 2$ então $n^2 \equiv 2^2 = 4$

Se $n \equiv 3$ então $n^2 \equiv 3^2 = 9 \equiv 0$

Se $n \equiv 4$ então $n^2 \equiv 4^2 = 16 \equiv 7$

Se $n \equiv 5$ então $n^2 \equiv 5^2 = 25 \equiv 7$

Se $n \equiv 6$ então $n^2 \equiv 6^2 = 36 \equiv 0$

Se $n \equiv 7$ então $n^2 \equiv 7^2 = 49 \equiv 4$

Se $n \equiv 8$ então $n^2 \equiv 8^2 = 64 \equiv 1$

Logo, não é possível que n seja um quadrado perfeito.

Problema 4.19. Prova que o número $30^{239} + 239^{30}$ não é primo.

Sugestão: mostra que o número é divisível por 31.

Resolução:

$30^{239} \equiv (-1)^{239} \equiv -1 \pmod{31}$

Como 31 é primo e $31 \nmid 239$, pelo pequeno teorema de Fermat temos que

$$239^{30} \equiv 1 \pmod{31}.$$

Assim,

$$30^{239} + 239^{30} \equiv -1 + 1 = 0 \pmod{31}.$$

Portanto, $31 | 30^{239} + 239^{30} \neq 31$ e por isso $30^{239} + 239^{30}$ não é primo.

Problema 4.20. Mostra que

$$a_t \times 10^t + a_{t-1} \times 10^{t-1} + \cdots + a_1 \times 10 + a_0 \equiv a_1 \times 10 + a_0 \pmod{4}$$

Resolução:

Portanto, o critério de divisibilidade por 4 diz: qualquer número natural é divisível por 4 se e só se o número formado pelos seus dois últimos algarismos for divisível por 4. Por exemplo, o número 769871532 é divisível de 4 porque 32 é divisível por 4.

Problema 4.21. O último algarismo do quadrado de um número natural n é igual a 6. Prova que o algarismo das dezenas é ímpar.

Resolução:

Começemos por observar que para todo k, $(2k)^2 = 4k^2$ é um número par, logo o seu último algarismo também é par; e que $(2k+1)^2 = 4k^2 + 4k + 1$ é um número ímpar, logo o seu último algarismo é ímpar.

Como o último algarismo de n^2 é igual a 6 então n é par.

O quadrado de qualquer número par é divisível por 4, pois $4 = 2^2$. Assim, pelo critério de divisibilidade por 4, sabemos que os últimos dois algarismos de n é divisível por 4.

Existem as seguintes possibilidades para os dois últimos algarismos de n: 06, 16, 26, 36, 46, 56, 66, 76, 86 e 96. Destas dez possibilidades, apenas 16, 36, 56, 76, e 96 são múltiplos de 4, e em todos os casos o algarismo das dezenas é ímpar.

Problema 4.22. Determina todos os primos p tais que $p^2 + 11$ tem exactamente seis divisores distintos (incluindo 1 e o próprio número).

Resolução:

Se $p \neq 3$, pelo pequeno teorema de Fermat, $p^2 \equiv 1 \pmod 3$. Por isso $p^2 + 11 \equiv 12 \equiv \equiv 0 \pmod 3$, isto é, $3|(p^2 + 11)$. Analogamente, se $p \neq 2$, pelo teorema de Euler, $p^2 \equiv 1 \pmod 4$, e por isso $p^2 + 11 \equiv 12 \equiv 0 \pmod 4$, isto é, $4|(p^2 + 11)$.

Assim, para $p \neq 2, 3$ vem que $12|(p^2 + 11)$. Como 12 tem seis divisores $(1, 2, 3, 4, 6$ e $12)$ e $\underbrace{p}_{>1}{}^2 + 11 > 12$, então $p^2 + 11$ tem de ter mais do que seis divisores.

Portanto, falta verificar os casos em que $p = 2$ e $p = 3$.

Se $p = 2$, então $p^2 + 11 = 15$, que tem apenas quatro divisores $(1, 3, 5$ e $15)$. Se $p = 3$, então $p^2 + 11 = 20$, que, de facto, tem seis divisores $(1, 2, 4, 5, 10$ e $20)$. Por isso, apenas $p = 3$ é solução do problema.

Problema 4.23. Sabendo que 2^{29} é um número com nove algarismos distintos, sem calcular o valor do número, determina qual dos dez algarismos está a faltar.

Resolução:

Vejamos que um número constituído pelos dez algarismos, de 0 a 9, é um múltiplo de 9, pois $0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45 \equiv 0 \pmod 9$.

Logo, para sabermos qual o algarismo em falta, basta saber qual o resto da divisão de 2^{29} por 9.

Pelo teorema de Euler, como 9 e 2 são coprimos e $\varphi(9) = \varphi(3^2) = 3^2\left(1 - \frac{1}{3}\right) = 6$

então $2^6 \equiv 1 \pmod 9$. Logo, $2^{29} = (2^6)^4 \cdot 2^5 \equiv 32 \equiv 5 \pmod 9$

Portanto, a soma dos algarismos do número 2^{29} é menor do que 45 e tem resto igual a 5 quando dividido por 9, ou seja, é igual a $36 + 5 = 41$.

Como $45 - 41 = 4$, o algarismo em falta é o 4.

Neste caso, é possível verificar que de facto $2^{29} = 536870912$.

Problema 4.24. Seja n um número natural que não é divisível por 17. Mostra que n^8+1 ou n^8-1 é divisível por 17.

Resolução:

Pelo pequeno teorema de Fermat, sabemos que $n^{16} \equiv 1 \pmod{17}$.

Como $(n^8+1)(n^8-1) = n^{16}-1 \equiv 0 \pmod{17}$, então um dos factores, n^8+1 ou n^8-1, é divisível por 17.

Problema 4.25. Seja $p \geq 7$ um número primo. Mostra que o número $11\ldots1$ com $p-1$ algarismos iguais a 1, é divisível por p.

Resolução:

Como $\underbrace{99\ldots9}_{n \text{ noves}} = 10^n - 1$ temos que

$$\underbrace{11\ldots1}_{p-1 \text{ uns}} = \frac{10^{p-1}-1}{9}$$

p e 10 são coprimos, pois $p \geq 7$ e $10 = 2 \times 5$. Logo, pelo pequeno teorema de Fermat $10^{p-1} \equiv 1 \pmod{p}$.

Portanto, em módulo p obtemos

$$\underbrace{11\ldots1}_{p-1 \text{ uns}} = \frac{10^{p-1}-1}{9} \equiv \frac{1-1}{9} = 0$$

isto é, p divide o número $\underbrace{11\ldots1}_{p-1 \text{ uns}}$.

Problema 4.26. Determina o último algarismo (alagrismo das unidades) dos números:

a) $3^{1001}7^{1002}13^{1003}$ **b)** $\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1001 \text{ setes}}$

Resolução:

Em ambas as alíneas basta determinar o resto da divisão de cada um dos números por 10.

a) Podemos utilizar o teorema de Euler pois 10 é coprimo com 3, com 7 e com 13.

$$\varphi(10) = \varphi(2 \times 5) \underbrace{=}_{\substack{2 \text{ e } 5 \\ \text{coprimos}}} \varphi(2)\varphi(5) = 4$$

Então,

$$3^4 \equiv 7^4 \equiv 13^4 \equiv 1 \pmod{10}.$$

Assim,

$$3^{1001} = (3^4)^{250} \times 3 \equiv 3 \pmod{10}$$
$$7^{1002} = (7^4)^{250} \times 7^2 \equiv -1 \pmod{10}$$
$$13^{1013} = (13^4)^{250} \times 13^3 \equiv -3 \pmod{10}$$

Portanto, $3^{1001}7^{1002}13^{1003} \equiv 3 \times (-1) \times (-3) = 9 \pmod{10}$.

b) Pela alínea **a)** vimos que $\varphi(10) = 4$, logo interessa-nos saber qual o resto da divisão de $\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1000 \text{ setes}}$ por 4.

Como $\varphi(4) = \varphi(2^2) = 2$ e 7 é coprimo com 4, temos que $7^2 \equiv 1 \pmod 4$ e por isso $7^{2k} \equiv 1 \pmod 4$ para todo k natural. Logo, $7^{2k+1} = 7^{2k} \cdot 7 \equiv 1 \cdot 3 = 3 \pmod 4$.

Assim, $\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1000 \text{ setes}} \equiv 3 \pmod 4$ e obtemos

$$\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1001 \text{ setes}} \equiv 7^3 \equiv 3 \pmod{10}$$

Problema 4.27. Determina os últimos três algarismos do número $2003^{2002^{2001}}$.

Resolução:

Neste caso é necessário determinar o resto da divisão de $2003^{2002^{2001}}$ por 1000.

Temos que

$$\underbrace{2003}_{\equiv 3}^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}$$

Como 3 e 1000 são coprimos, podemos aplicar o teorema de Euler e por isso vamos calcular $\varphi(1000)$.

$$\varphi(1000) = \varphi(2^3 \times 5^3) \underset{\substack{\underbrace{\quad}\\ 2 \text{ e } 5 \\ \text{coprimos}}}{=} \varphi(2^3)\varphi(5^3) = 2^3\left(1 - \frac{1}{2}\right) \cdot 5^3\left(1 - \frac{1}{5}\right) = 400$$

Logo, é necessário calcular 2002^{2001} ou 2^{2001} módulo 400.

Como $400 = 16 \times 25$ e $16 = 2^4$ divide 2^{2001}, temos que $2^{2001} \equiv 16k \pmod{400}$, para algum k natural.

Mas,

$$2^{2001} = 2^4 \cdot 2^{1997} \equiv 16k = 2^4 k \pmod{400}$$

Logo, $2^{1997} \equiv k \pmod{25}$.

Novamente, utilizando o teorema de Euler, como $\varphi(25) = 5^2\left(1-\frac{1}{5}\right) = 20$, temos

$$2^{1997} = (2^{20})^{99} \cdot 2^{17} \equiv 2^{17} = \underbrace{2^7}_{\equiv 3} \cdot \underbrace{2^7}_{\equiv 3} \cdot 2^3 \equiv 3 \times 3 \times 8 = 72 \equiv 22 \pmod{25}$$

Portanto, $k \equiv 22$ e por isso $2002^{2001} \equiv 2^{2001} \equiv 16k \equiv 16 \times 22 = 352 \pmod{400}$.

Logo,

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \equiv 3^{352} \pmod{1000}$$

Ao escrever $3^{352} \equiv 9^{176} = (10-1)^{176}$ é possível aplicar o Binómio de Newton

$$(x+y)^n = \sum_{k=0}^{n} x^{n-k}y^k$$

Como todos os termos múltiplos de 10^t, com $t \geq 3$ são congruentes com zero, módulo 1000, temos

$$(10-1)^{176} \equiv \binom{176}{2} \cdot 10^2 - \binom{176}{1} \cdot 10 + 1^{176} \equiv 0 - 760 + 1 \equiv 241 \pmod{1000}$$

Problema 4.28. Seja p um número primo.

a) Mostra que se p é diferente de 3 então número $111\ldots11$ (p algarismos 1) não é divisível por p.

b) Prova que se $p > 5$ então o número $111\ldots11$ ($p-1$ algarismos 1) é divisível por p.

Resolução:

a) $\underbrace{111\ldots11}_{p \text{ uns}} = \frac{(10^p-1)}{9}$

Pelo pequeno teorema de Fermat $10^p \equiv 10 \pmod{p}$ (repara que $p \neq 3$ e por isso existe a possibilidade de p dividir 10).

Logo, $10^p - 1 \equiv 10 - 1 \equiv 9 \pmod{p}$, ou seja, $\underbrace{111\ldots11}_{p \text{ uns}}$ não é divisível por p pois

$$\underbrace{111\ldots11}_{p \text{ uns}} = \frac{(10^p-1)}{9} \equiv \frac{9}{9} = 1 \pmod{p}.$$

b) $\underbrace{111\ldots11}_{p-1 \text{ uns}} = \frac{(10^{p-1}-1)}{9}$

Pelo pequeno teorema de Fermat $10^{p-1} \equiv 1 \pmod{p}$ pois $p > 5$.

Logo, $10^{p-1} - 1 \equiv 0 \pmod{p}$, ou seja, $\underbrace{111\ldots11}_{p-1 \text{ uns}}$ é divisível por p pois

$$\underbrace{111\ldots11}_{p \text{ uns}} = \frac{(10^{p-1}-1)}{9} \equiv \frac{0}{9} = 0 \pmod{p}.$$

Problema 4.29. Seja n um número natural. Prova que $3^{2^n}+1$ é divisível por 2, mas não é divisível por 4.

Resolução:

$\underbrace{3}_{\equiv 1}^{2^n}+1 \equiv 1^{2^n}+1 = 2 \equiv 0 \pmod 2$ logo $2 | 3^{2^n}+1$

$\underbrace{3}_{\equiv -1}^{2^n}+1 \equiv \underbrace{(-1)^{2^n}}_{\text{é sempre par}}+1 = 1+1 \equiv 2 \pmod 4$ logo $2 \nmid 3^{2^n}+1$.

Problema 4.30. Encontra n tal que $2^n \parallel 3^{1024}-1$.

Resolução:

Vejamos primeiro que $2^{10} = 1024$.

Assim, temos que

$$3^{1024}-1 = \underbrace{3^{2^{10}}}_{\left(3^{2^9}\right)^2} - \underbrace{1}_{1^2} = \left(3^{2^9}+1\right)\left(3^{2^9}-1\right) = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\left(3^{2^8}-1\right) =$$

$$= \cdots = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\left(3^{2^7}+1\right)\ldots\left(3^{2^1}+1\right)\left(3^{2^0}+1\right)(3-1)$$

Pelo problema **4.29** verificamos que $3^{2^k}+1$ é divisível por 2 mas não é divisível por 4 para todo $k \geq 1$. Logo, no produto $\left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\left(3^{2^7}+1\right)\ldots\left(3^{2^1}+1\right)$ existem 9 factores iguais a 2.

Como $\left(3^{2^0}+1\right)(3-1) = 4 \times 2 = 2^3$, no total na factorização de $3^{1024}-1$ existem $9+3 = 12$ factores iguais a 2.

Portanto, $2^{12} \parallel 3^{1024}-1$.

5. Colecção de problemas

Segue-se um conjunto de problemas com o objectivo de desafiar o aluno, permitindo a aplicação dos conhecimentos adquiridos nos capítulos anteriores.
As soluções ou sugestões de resolução destes problemas encontram-se no final do capítulo.

Problema 5.1. O número $15A$ é divisível por 6. Será verdade que A é divisível por 6?

Problema 5.2. O número $5^9 \cdot 3$ é divisível por 15? Será também divisível por 1125?

Problema 5.3. Dados os números $A = 2^8 \cdot 5^3 \cdot 7$ e $B = 2^5 \cdot 3 \cdot 5^7$ encontra o $\text{mmc}(A, B)$ e o $\text{mdc}(A, B)$.

Problema 5.4. Determina $\text{mdc}(2n + 13, n + 7)$.

Problema 5.5. Quantos zeros há no final da representação decimal do número $100!$?

Problema 5.6. Indica todos os números naturais que são solução da equação $x^2 - y^2 = 31$.
Sugestão: $x^2 - y^2 = (x - y)(x + y)$.

Problema 5.7. Encontra d o maior divisor do número 1001001001 tal que $d \leq 10000$.

Problema 5.8. Sem utilizar congruências, mostra que $n^2 + 1$ não é divisível por 3, para todo o n.

Problema 5.9. Sem utilizar congruências, qual o resto da divisão de 2^{100} por 3.

Problema 5.10. Sejam ab e ba dois números naturais de dois algarismos. Prova que a soma destes dois números é um número composto.

Problema 5.11. (Euler, 1770) Divide 100 em duas parcelas, sendo a primeira múltipla de 11 e a outra múltipla de 7.

Problema 5.12. Qual o último algarismo do número 777^{777}?

Problema 5.13. Qual o resto da divisão de 3^{1989} por 7.

Problema 5.14. Prova que $2222^{5555} + 5555^{2222}$divisível por 7.

Problema 5.15. Determina todos os naturais k tais que o número $\underbrace{11\ldots1}_{k \text{ uns}}$ não é um quadrado perfeito..

Problema 5.16. Seja n um número de cinco algarismos distintos, todos pares. Pode n ser um quadrado perfeito?

Problema 5.17. O número $a = \underbrace{20\ldots04}_{2004}$ é um quadrado perfeito?

Problema 5.18. Descobre o resto da divisão de 8^{900} por 29.

Problema 5.19. Sejam a, b, c, d algarismos distintos. Prova que o número representado por $cdcdcdcd$ não é divisível por $aabb$.

Problema 5.20. A soma de dois números algarismos a e b é divisível por 7. Mostra que o número representado por aba também é divisível por 7.

Problema 5.21. Seja n um número inteiro maior do que 3. Prova que $1! + 2! + \cdots + n!$ não pode ser uma potência perfeita.

5.1. Soluções/Sugestões

Problema 5.1. Não. Encontra um contra-exemplo.

Problema 5.2. A resposta às duas perguntas é não. Factoriza os números 15 e 1125.

Problema 5.3. $\text{mmc}(A,B) = 420000000$ e $\text{mdc}(A,B) = 4000$.

Problema 5.4. $\text{mdc}(2n+13, n+7) = 1$.

Problema 5.5. Repara que se um número tem n zeros no final da sua representação decimal, então é divisível por 10^n. O número $100!$ termina com 24 zeros.

Problema 5.6. $x = 16$ e $y = 15$.

Problema 5.7. Observa que $1001001001 = 7 \times 11 \times 13 \times (10^6 + 1)$ e escreve $(x^6 + 1)$ como o produto de dois polinómios de grau menor.

Problema 5.8. Analisa os restos da divisão de n por 3.

Problema 5.9. Começa por determinar os restos das divisões de 2^k por 3 para os primeiros valores de $k \in \mathbb{N}$. O resto é igual a 1.

Problema 5.10. Mostra que $ab + ba$ é múltiplo de 11.

Problema 5.11. Resolve a equação diofantina $100 = 11x + 7y$.

Problema 5.12. O último algarismo é igual a 7.

Problema 5.13. O é igual a 6.

Problema 5.14. Mostra que $2222^{5555} + 5555^{2222}$é congruente com zero, módulo 7.

Problema 5.15. O número dado é um quadrado perfeito apenas para $k = 1$. Mostra que $\underbrace{11\ldots1}_{k \text{ uns}} \equiv 3 \pmod 4$.

Problema 5.16. Mostra que $n \equiv 2 \pmod 9$.

Problema 5.17. Não. Mostra que $a \equiv 6 \pmod 9$.

Problema 5.18. Utiliza o pequeno teorema de Fermat. O resto é igual a 7.

Problema 5.19. Utilizando o critério de divisibilidade por 11, mostra que número $aabb$ é divisível por 11 e o número $cdcdcdcd$ não é.

Problema 5.20. $aba = 7(14a + b) + (3a + b)$

Problema 5.21. Visto que $1! + 2! + \cdots + n! \equiv 3 \pmod{10}$, então não pode ser quadrado perfeito, nem potência perfeita de expoente par. Para potências de expoente ímpar, verifica diretamente para $n < 9$ e depois mostra que para $n \geq 9$ o número $1! + 2! + \cdots + n!$ não é múltiplo de 27.

6. Referências bibliográficas

Andreescu, Titu; Andrica, Dorin; Feng, Zuming, *104 Number Theory Problems*, Boston, Birkhäuser, 2007

Burton, David. M, *Elementary Number Theory*, New York, McGraw-Hill, 2002

Burton, David. M, *The History of Mathematics: An Introduction*, New York, McGraw--Hill, 2006

Engel, Arthur, *Problem-Solving Strategies*, New York, Springer, 1998

Fomin; Dmitri; Genkin, Sergey; Itenberg, Llia *Mathematical Circles (Russian Experience)*, Hyderguda, Universities Press, 1998

Freitas, Pedro J., *Apontamentos da cadeira Teoria Elementar dos Números*, 2012

Hong-Bing, Yu, *Mathematical Olympiad Series (Vol. 2) – Problems of Number Theory in Mathematical Competitions*, Shanghai, East China normal University Press and World Scientific Publishing Co. Pte. Ltd., 2010

Krantz, Steven G., *Techniques of Problem Solving*, USA, American Mathematical Society, 1997

Zeitz, Paul, *The Art and Craft of Problem Solving*, USA, John Wiley & Sons, Inc., 2007